CA User Activity Reporting Module

Administration Guide

Versione 12.5.03

La presente documentazione, che include il sistema di guida in linea integrato e materiale distribuibile elettronicamente (d'ora in avanti indicata come "Documentazione"), viene fornita all'utente finale a scopo puramente informativo e può essere modificata o ritirata da CA in qualsiasi momento.

Questa Documentazione non può essere copiata, trasmessa, riprodotta, divulgata, modificata o duplicata per intero o in parte, senza la preventiva autorizzazione scritta di CA. Questa Documentazione è di proprietà di CA e non potrà essere divulgata o utilizzata se non per gli scopi previsti in (i) uno specifico contratto tra l'utente e CA in merito all'uso del software CA cui la Documentazione attiene o in (ii) un determinato accordo di confidenzialità tra l'utente e CA.

Fermo restando quanto enunciato sopra, se l'utente dispone di una licenza per l'utilizzo dei software a cui fa riferimento la Documentazione avrà diritto ad effettuare copie della suddetta Documentazione in un numero ragionevole per uso personale e dei propri impiegati, a condizione che su ogni copia riprodotta siano apposti tutti gli avvisi e le note sul copyright di CA.

Il diritto a stampare copie della presente Documentazione è limitato al periodo di validità della licenza per il prodotto. Qualora e per qualunque motivo la licenza dovesse cessare o giungere a scadenza, l'utente avrà la responsabilità di certificare a CA per iscritto che tutte le copie anche parziali del prodotto sono state restituite a CA o distrutte.

NEI LIMITI CONSENTITI DALLA LEGGE VIGENTE, LA DOCUMENTAZIONE VIENE FORNITA "COSÌ COM'È" SENZA GARANZIE DI ALCUN TIPO, INCLUSE, IN VIA ESEMPLIFICATIVA, LE GARANZIE IMPLICITE DI COMMERCIABILITÀ, IDONEITÀ A UN DETERMINATO SCOPO O DI NON VIOLAZIONE DEI DIRITTI ALTRUI. IN NESSUN CASO CA SARÀ RITENUTA RESPONSABILE DA PARTE DELL'UTENTE FINALE O DA TERZE PARTI PER PERDITE O DANNI, DIRETTI O INDIRETTI, DERIVANTI DALL'UTILIZZO DELLA DOCUMENTAZIONE, INCLUSI, IN VIA ESEMPLICATIVA E NON ESAUSTIVA, PERDITE DI PROFITTI, INTERRUZIONI DELL'ATTIVITÀ, PERDITA DEL GOODWILL O DI DATI, ANCHE NEL CASO IN CUI CA VENGA ESPRESSAMENTE INFORMATA IN ANTICIPO DI TALI PERDITE O DANNI.

L'utilizzo di qualsiasi altro prodotto software citato nella Documentazione è soggetto ai termini di cui al contratto di licenza applicabile, il quale non viene in alcun modo modificato dalle previsioni del presente avviso.

Il produttore di questa Documentazione è CA.

Questa Documentazione è fornita con "Diritti limitati". L'uso, la duplicazione o la divulgazione da parte del governo degli Stati Uniti è soggetto alle restrizioni elencate nella normativa FAR, sezioni 12.212, 52.227-14 e 52.227-19(c)(1) - (2) e nella normativa DFARS, sezione 252.227-7014(b)(3), se applicabile, o successive.

Copyright © 2011 CA. Tutti i diritti riservati. Tutti i marchi, i nomi commerciali, i marchi di servizio e i loghi citati nel presente documento sono di proprietà delle rispettive aziende.

Riferimenti ai prodotti CA

Questo documento è valido per i seguenti prodotti di CA:

- CA Access Control
- CA Audit
- CA ACF2™
- CA Directory
- CA Embedded Entitlements Manager (CA EEM)
- CA Enterprise Log Manager
- CA Identity Manager
- CA IT Process Automation Manager (CA IT PAM)
- CA NSM
- CA Security Command Center (CA SCC)
- CA Service Desk
- CA SiteMinder®
- CA Spectrum®
- CA Top Secret®

Contattare il servizio di Supporto tecnico

Per l'assistenza tecnica in linea e un elenco completo delle sedi, degli orari del servizio di assistenza e dei numeri di telefono, contattare il Supporto tecnico visitando il sito Web all'indirizzo http://www.ca.com/worldwide.

Modifiche apportate alla documentazione

Dall'ultima versione della presente documentazione, sono state aggiornate le seguenti aree: integrazioni e connettori.

Gli argomenti interessati sono i seguenti:

- Integrazioni e connettori:
  - Impostazione della CPU del connettore: nuovo argomento riguardante la configurazione del rallentamento della CPU.

Ulteriori informazioni:

Impostazione della CPU del connettore (a pagina 616)

Sommario

Capitolo 1: Introduzione 19

Informazioni sulla Guida 19

Capitolo 2: Account utente 23

Attività di auto-amministrazione 23
- Sblocco di un account utente 24
- Modificare la propria password 25

Attività associate ai ruoli 25
- Operazioni del revisore 26
- Attività dell'analista 28
- Attività dell'amministratore 29

Configurazione degli account con impostazioni predefinite 37
Creazione di un gruppo globale 38
Creazione di un utente globale 39
Assegnazione di un ruolo a un utente globale 40
Modalità di gestione degli account utente di riferimento 42
Linee guida per l'attivazione di un utente 42
Modifica di un account utente 43
Ripristino di una password utente 45
Eliminazione di un account utente 46

Capitolo 3: Criteri 47

Introduzione ai criteri 48
Criteri di accesso predefiniti 48
- Esaminare i criteri per tutti gli utenti. 49
- Esaminare i criteri per i revisori 53
- Esaminare i criteri per gli analisti 55
- Esaminare i criteri per gli amministratori 58
- Criteri di accesso per i prodotti registrati 60

Eseguire il backup di tutti i criteri di accesso 61
Ripristino dei criteri di accesso 65

Capitolo 4: Ruoli e criteri predefiniti 69

Linee guida per la creazione di criteri 69
Tipi di criteri di accesso di CALM 73
Risorse ed azioni 76
Risorse CALM e cartelle EEM 79
Risorse globali e Funzionalità CA EEM 82
Pianificazione del ruolo utente 83
Configurazione di ruoli utente personalizzati e criteri di accesso 84
Creazione di un gruppo utente delle applicazioni (ruolo) 87
Come garantire l'accesso ruolo personalizzato a CA User Activity Reporting Module 88
Aggiunta di un'identità a un criterio esistente 90
Creazione di un criterio di accesso a CALM 91
Creazione di un criterio di scoping 94
Creazione di un criterio basato su un criterio esistente 98
Verifica di un nuovo criterio 100
Creazione di un criterio per un gruppo utente dinamico 101
Creazione di un filtro di accesso 103
Gestione di account utente e criteri di accesso 104
Creazione di un calendario 105
Aggiunta di un calendario a un criterio 106
Esempio: limitazione dell'accesso ai giorni lavorativi 107
Esportazione dei criteri di accesso 109
Eliminazione di un criterio personalizzato 109
Eliminazione di filtri di accesso e criteri di obbligo 110
Esempio: consentire a chi non è amministratore di gestire gli archivi 111
Limitazione dell'accesso ai dati per un utente: scenario Win-Admin 115
Passaggio 1: creazione dell'utente Win-Admin 117
Passaggio 2: aggiunta di Win-Admin al criterio di accesso all'applicazione di CALM 118
Passaggio 3: creazione del criterio di accesso al sistema Win-Admin 119
Passaggio 4: creazione di filtri di accesso ai dati Win-Admin 123
Passaggio 5: accesso come utente Win-Admin 126
Passaggio 6: estensione delle azioni garantite 128
Limitazione dell'accesso a un ruolo: scenario per analisti PCI 129
Passaggio 1: pianificazione del ruolo e dei criteri da creare 131
Passaggio 2: creazione del ruolo Analista PCI 132
Passaggio 3: aggiunta dell'analista PCI al criterio di accesso all'applicazione CALM. 133
Passaggio 4: aggiunta dell'analista PCI ai criteri esistenti 133

Passaggio 5: creazione di un criterio basato sul criterio di visualizzazione-modifica rapporti per analisti 134
Passaggio 6: assegnazione del ruolo di analista PCI a un utente 136
Passaggio 7: accesso come analista PCI e valutazione dell'accesso 136
Criteri di esempio per le integrazioni personalizzate 138
Criteri di esempio per le regole di soppressione e riepilogo 139

Capitolo 5: Servizi e adapter CA 143

Attività servizi 144
Eliminazione di un host di servizio 145
Modificare le configurazioni globali 145
Modifica di una configurazione di servizio globale 148
Modifica di una configurazione di servizio locale 149
Configurazioni di servizio 150
Considerazioni sul servizio di avviso 151
Considerazioni sul servizio di correlazione 158
Considerazioni sul deposito eventi di log 159
Considerazioni sul servizio incidenti 164
Considerazioni su ODBC Server 165
Considerazioni sul servizio di rapporto 166
Considerazioni sul servizio test della regola 168
Considerazioni sulla sottoscrizione 168
Servizio di stato del sistema 173
Attività di configurazione degli adapter CA 173
Modifica di una configurazione adapter globale 174
Modifica di una configurazione adapter locale 175
Visualizzazione degli eventi adapter di automonitoraggio 176
Visualizzazione dello stato degli adapter 177
Considerazioni sul servizio SAPI 178
Considerazioni su iTechnology Event Service 180
Attività di Stato del sistema 180
Creare un file di diagnostica di supporto 181
Riavviare un server host 182
Riavviare i servizi ELM. 182
Controllare lo stato e la versione dei servizi 183
Controllare gli eventi di automonitoraggio dello stato del sistema 183

Capitolo 6: Archiviazione dei registri 185

Informazioni sull'archiviazione dei log 186
Stati del database del registro eventi 188
Backup e ripristino automatici 191
Controlli di integrità dei dati 192
Funzionamento dei controlli di integrità dei dati per eventi non elaborati 193
Impostazione dei controlli di integrità dei dati 194
Firma dei database in quarantena 197
Rotazione delle chiavi 197
Importazione di chiavi 198
Esportazione di chiavi 198
Configurazione dell'autenticazione non interattiva per il ripristino 199
Esempio: Configurazione dell'autenticazione dal server di archiviazione remoto ad un punto di ripristino 200
Esempio: Configurazione dell'autenticazione da un server di archiviazione ad un server di rapporto 202
Invio di query al catalogo archiviazioni 205
Ripristino dei file archiviati automaticamente 207
Script per il ripristino di database archiviati 208
Esecuzione manuale del backup dei database archiviati 210
Identificazione dei database non sottoposti a backup 211
Esecuzione dei backup 212
Registrazione dei backup 213
Ripristino manuale degli archivi dall'archivio registro eventi di origine 214
Preparazione del ripristino dei database archiviati 215
Trasferimento dei database archiviati su una directory di archiviazione 218
Ripristino dei file archiviati manualmente 219
Verifica del ripristino 221
Ripristino manuale degli archivi dal nuovo archivio registro eventi 221
Configurazione del numero massimo di giorni di archiviazione per gli archivi ripristinati 223
Aggiunta di database ripristinati al catalogo 224
Monitoraggio di backup e ripristino di LMArchive 225

Capitolo 7: Sottoscrizione 227

Aggiornamento a CA User Activity Reporting Module versione 12.5 attraverso la sottoscrizione 227
Visualizzazione dello stato di sottoscrizione globale 229
Visualizzazione dello stato di sottoscrizione di un server 230
Modifica della configurazione di sottoscrizione globale 232

Modifica della configurazione di sottoscrizione locale di un server 233
Download e selezione dei moduli per la sottoscrizione non in linea 235
Informazioni sugli aggiornamenti su richiesta 237
Avviare un aggiornamento su richiesta 239
Spazio libero su disco per gli aggiornamenti 241
Informazioni sulle chiavi pubbliche di sottoscrizione 242
Automonitoraggio degli eventi per la sottoscrizione 242
Monitoraggio degli eventi di sottoscrizione 243
Visualizzazione dei dettagli degli eventi di sottoscrizione 246
Applicazione degli aggiornamenti di sottoscrizione agli agenti ed ai connettori 248

Capitolo 8: Filtri e profili 251

Capitolo 9: Filtri globali e locali 253

Informazioni sui filtri semplici 254
Impostazione di un filtro semplice 255
Informazioni sui filtri profilo 256
Modalità di creazione di un profilo 257
Aprire l'impostazione guidata profilo 258
Aggiunta di dettagli al profilo 258
Creazione dei Filtri dati 259
Creazione di Filtri tag 260
Importazione di un profilo 261
Esportazione di un profilo 262
Impostazione di un profilo 262
Creazione di un filtro globale 263
Configurazione delle impostazioni globali delle query 265
Modifica di un filtro globale 266
Rimozione di un filtro globale 266
Creazione di un filtro locale 267
Modifica di un filtro locale 268
Rimozione di un filtro locale 268

Capitolo 10: Query e rapporti 269

Informazioni su query e rapporti 270
Attività relative ai tag 273

Capitolo 11: Formato data/ora 274

Formati data/ora supportati 275
Modifica del formato data/ora 277
Visualizzazione di una query 278
Visualizzazione di un rapporto 279
Disattivazione dell'opzione Mostra rapporto selezionato 281
Esempio: esecuzione di rapporti PCI 282
Visualizzazione dell'elenco dei rapporti con il tag PCI 282
Ricerca di rapporti per un controllo PCI DDS specifico 283
Lavorare con un solo rapporto PCI 286
I prompt 287
Utilizzo del Prompt di connettore 289
Utilizzo del prompt Host 292
Utilizzo del prompt IP 295
Utilizzo del prompt di Nome registro 298
Utilizzo del prompt Porta 300
Utilizzo del prompt Utente 302
Come creare una query 305
Apertura della procedura guidata Progettazione query 306
Aggiunta di dettagli sulla query 307
Aggiunta di colonne di query 309
Aggiunta di colonne di query ODBC 311
Impostazione dei filtri della query 314
Modalità di impostazione delle condizioni risultato 318
Creazione di una visualizzazione di query 323
Aggiunta di un rapporto drill-down 324
Modifica di una query 325
Eliminazione di una query personalizzata 325
Disattivazione dell'opzione Mostra query selezionata 326
Esportazione e importazione delle definizioni delle query 326
Esportazione delle definizioni di query 327
Importazione delle definizioni di query 328
Modalità di creazione di un rapporto 329
Apertura della procedura guidata Progettazione rapporto 329
Aggiunta di dettagli al rapporto 330
Progettazione del layout rapporto 332
Esempio: creazione di un rapporto da query esistenti 333
Esempio: impostazione della federazione e dei rapporti federati 337

Modifica di un rapporto 342
Eliminazione di un rapporto personalizzato 342
Esempio: eliminazione dei rapporti giornalieri con più di 30 giorni 343
Esportazione delle definizioni dei rapporti 345
Importazione delle definizioni dei rapporti 346
Preparazione all'utilizzo di rapporti dotati di elenchi con chiave 347
Abilitare l'importazione di valori dinamici 348
Approcci alla manutenzione degli elenchi con chiave 352
Creare i valori chiave per i rapporti predefiniti 360
Visualizzare un rapporto utilizzando un elenco con chiave 364

Capitolo 12: Avvisi 365

Informazioni relative agli avvisi 366
Utilizzo delle query con il tag Avviso 367
Identificare altre query da utilizzare per gli avvisi. 369
Personalizzare le query per gli avvisi 370
Identificare il filtro semplice per gli eventi di elevata gravità 371
Creare una query per recuperare solo gli eventi gravi 373
Personalizzare le query in modo da recuperare solo gli eventi gravi 375
Considerazioni relative agli avvisi 381
Utilizzare i processi CA IT PAM di output di evento/avviso 384
Informazioni sui processi CA IT PAM di output di evento/avviso 385
Importazione del processo di output di evento/avviso campione 393
Linee guida per la creazione di un processo di output di evento/avviso 401
Raccogliere informazioni per l'integrazione di CA IT PAM 405
Esempio: eseguire un processo di output di evento/avviso con i risultati della query selezionata 409
Progettare le query di eventi da inviare al processo di output di evento/avviso 413
Esempio: inviare un avviso che esegue un processo IT PAM per riga 415
Esempio: inviare un avviso che esegua un processo di IT PAM per query 420
Modalità di utilizzo delle trap SNMP 423
Informazioni sui trap SNMP 424
Esempi di filtri semplici per gli avvisi da inviare come trap 424
Informazioni sui file MIB 426
Processo di utilizzo dei trap SNMP 443
Configurare l'integrazione con una destinazione di trap SNMP 445
Preparare CA Spectrum per ricevere le trap SNMP dagli avvisi 446
Esempio: avvisare CA Spectrum delle modifiche alla configurazione 451

Preparazione di CA NSM per la ricezione di trap SNMP dagli avvisi 456
Esempio: Segnalazione di modifiche della configurazione a CA NSM 460
Creazione di un alert 470
Apertura della procedura guidata di pianificazione di avvisi 471
Selezione di una query di avviso 472
Impostazione dei parametri di pianificazione di un processo di avviso 473
Impostare le destinazioni di notifica 474
Definizione della destinazione della query del processo di avviso 479
Esempio: creazione di un avviso per Spazio su disco insufficiente 479
Esempio: creazione di un avviso per un evento di automonitoraggio 484
Esempio: inviare un messaggio di posta elettronica all'amministratore quando si arresta il flusso degli eventi 487
Configurazione della memorizzazione degli avvisi 491
Esempio: creazione di un avviso per Business_Critical_Sources 491
Modifica di un avviso 494
Abilitare o disabilitare gli avvisi 494
Eliminazione di un avviso 495

Capitolo 13: Rapporti pianificati 497

Visualizzazione di un rapporto generato 497
Come filtrare i rapporti 498
Annotazioni a un rapporto generato 499
Abilitare e disabilitare i processi di rapporto pianificati 500
Pianificazione di un processo di rapporto 501
Apertura della procedura guidata Pianificazione rapporto 502
Selezione di un modello di rapporto 503
Impostazione dei parametri di pianificazione 505
Selezione delle impostazioni relative a formato e notifiche 506
Scelta della destinazione delle query di un rapporto 507
Esempio: pianificazione di rapporti con un tag comune 507
Esempio: invio tramite posta elettronica di rapporti PCI in formato PDF 511
Modifica di un processo di rapporto pianificato 512
Abilitare e disabilitare i processi di rapporto pianificati 513
Eliminazione di un processo di rapporto pianificato 514
Eventi di automonitoraggio 514
Visualizzazione di un evento di automonitoraggio 515

Capitolo 14: Soppressione e riepilogo 517

Versioni dei componenti per il perfezionamento degli eventi 517
Attività relative alle regole per la soppressione e il riepilogo 518
Effetti della regola di soppressione 519
Modalità di creazione di una regola per la soppressione 520
Modalità di creazione di una regola per il riepilogo 526
Applicazione di una regola di soppressione o riepilogo 533
Come applicare regole di soppressione e riepilogo ai componenti degli agenti 533
Copia di una regola di soppressione o riepilogo 537
Modifica di una regola per la soppressione o il riepilogo 538
Eliminazione di una regola per la soppressione o il riepilogo 539
Importazione di una regola per la soppressione o il riepilogo 540
Esportazione di una regola per la soppressione o il riepilogo 541
Creazione di una regola di soppressione per l'evento Windows 560 542

Capitolo 15: Mapping e Analisi 545

Stati evento 546
Attività relative a regole di mapping e analisi 548
Modalità di creazione di un file di analisi del messaggio 548
Apertura della procedura guidata file di parsing 550
Definizione dei dettagli del file 550
Caricamento di eventi campione 552
Aggiungi campi globali 553
Creazione di un filtro di corrispondenza preliminare 554
Creazione di un filtro di analisi 556
Analisi del file XMP 567
Modalità di creazione di un file di mapping dei dati 568
Apertura della procedura guidata di mapping di file 570
Fornire dettagli dei file 571
Fornitura degli eventi campione 571
Impostazione di mapping diretti 573
Impostazione dei mapping di funzione 574
Impostazione del mapping di funzione di concatenazione 576
Impostazione dei mapping condizionali 577
Impostazione dei mapping di blocco 579
Esecuzione dell'analisi del mapping 581
Attività delle regole di inoltro eventi 581
Come creare regole di inoltro eventi. 582

Informazioni sugli Eventi syslog inoltrati 588
Modifica di una regola di inoltro 589
Eliminazione di una regola di inoltro 590
Importazione di una regola di inoltro 590
Esportazione di una regola di inoltro 591

Capitolo 16: Integrazioni e connettori 593

Attività relative a integrazioni e connettori 593
Modalità di creazione di un'integrazione 595
Apertura della procedura guidata di integrazione 596
Aggiunta di componenti dell'integrazione 597
Applicare le regole di soppressione e riepilogo 598
Impostazione delle configurazioni predefinite 599
Impostazione delle configurazioni del registro file 600
Modalità di creazione di un listener syslog 602
Apertura della procedura guidata listener 603
Aggiunta di componenti listener 604
Applicazione delle regole di soppressione e riepilogo 605
Impostazione delle configurazioni predefinite 606
Aggiunta di un fuso orario syslog 608
Creazione di una nuova versione di integrazione 609
Eliminazione di un'integrazione 610
Esportazione e importazione delle definizioni delle integrazioni 610
Importazione delle definizioni delle integrazioni 611
Esportazione delle definizioni delle integrazioni 611
Modalità di creazione di un connettore 612
Apertura della creazione guidata del connettore 613
Aggiunta di dettagli al connettore 613
Applicazione delle regole di soppressione e riepilogo 614
Impostazione della configurazione di un connettore 615
Impostazione della CPU del connettore 616
Visualizzazione di un connettore 617
Visualizzazione di una guida per il connettore 617
Modifica di un connettore 618
Informazioni sulle configurazioni salvate 619
Creazione di una configurazione salvata 620
Come configurare i connettori in blocco 621
Aprire la procedura guidata Configura origini di raccolta. 622

Selezionare Dettagli origine 623
Applicazione delle regole di soppressione 624
Applicazione di regole di riepilogo 624
Configurazione connettore 625
Selezionare gli agenti e mappare le origini 626
Aggiornamento delle configurazioni di più connettori 627

Capitolo 17: Correlazione eventi e Gestione incidenti 629

Capitolo 18: Attività delle regole di correlazione 631

Informazioni sulle regole di correlazione 632
Utilizzo di regole di correlazione predefinite 633
Utilizzo degli elenchi con chiave con le regole di correlazione 637
Esempio: creazione di un file CSV per il test 638
Informazioni sulle notifiche di incidente 638
Come progettare e applicare le notifiche di incidente 640

Capitolo 19: Attività di gestione incidenti 645

Visualizzazione di dettagli su un incidente 646

Capitolo 20: Attività dei profili di raccolta evento 647

Creazione di un profilo di raccolta evento 647
Impostazione delle informazioni relative al profilo di raccolta 648
Applicazione delle regole di soppressione e riepilogo 649
Configurazione del profilo di raccolta 650

Capitolo 21: Agenti 651

Pianificazione dell'installazione di un agente 652
Pianificazione della configurazione degli agenti 654
Pianificazione della raccolta registri diretta 656
Pianificazione della raccolta registri priva di agenti 658
Pianificazione della raccolta di registri basata sugli agenti 658
Selezione del livello da configurare 659
Attività di gestione agente 660
Aggiornamento della Chiave di autenticazione agente 661
Download dei file binari agente 662
Configurazione di un agente 662

Gestione di un file di configurazione manomesso 665
Visualizzare il dashboard di agente 666
Visualizzazione e controllo dello stato di agenti o connettori 667
Modalità di creazione di un gruppo di agenti 669
Apertura della procedura guidata Gruppo di agenti 669
Aggiunta dei dettagli del gruppo di agenti 670
Aggiunta di agenti ad un gruppo di agenti 671
Modalità di configurazione della gestione agente 672
Apertura della procedura guidata di assegnazione Server Log Manager 673
Selezione degli agenti di destinazione 674
Selezione dei server Log Manager 675
Modalità di protezione degli agenti dalle conseguenze dei cambi di indirizzo IP dei server 676
Garantire la disponibilità dei server con indirizzi IP dinamici 677
Garantire la disponibilità dei server durante la riassegnazione degli indirizzi IP statici 677
Modalità di applicazione degli aggiornamenti di sottoscrizione 679
Apertura della procedura guidata Elenco aggiornamenti 680
Selezione degli agenti o dei connettori da aggiornare 681
Aggiornamento delle versioni di integrazione dell'agente o del connettore 682
Creazione di un file di diagnosi agente per il Supporto 683

Capitolo 22: Certificati personalizzati 685

Implementazione di certificati personalizzati 685
Aggiunta del Certificato radice attendibile al server di gestione CA User Activity Reporting Module 686
Aggiunta del Certificato radice attendibile a tutti gli altri server CA User Activity Reporting Module 688
Aggiunta del nome comune di certificato ad un criterio di accesso 689
Distribuzione dei nuovi certificati 690

Appendice A: Funzionalità di accessibilità 693

Modalità di accessibilità 693
Controlli di accessibilità 693
Impostazioni CA User Activity Reporting Module della lingua di visualizzazione 694
Localizzazione manuale di CA User Activity Reporting Module 695

Appendice B: Accesso agli eventi raccolti con ODBC e JDBC 697

Informazioni sull'accesso ODBC/JDBC in CA User Activity Reporting Module 697

Creazione di query ODBC e JDBC da utilizzare con CA User Activity Reporting Module 698
Limitazioni del supporto SQL 698
Funzioni SQL supportate 699
Elaborazione delle query 700
Alias delle colonne di risultati 701
Limiti risultato 701
Codici di errore specifici di CA User Activity Reporting Module 701
Esempio: utilizzare un filtro di accesso per limitare i risultati ODBC 702
Esempio: preparazione all'utilizzo dei client ODBC e JDBC con Crystal Reports 704
Creazione di un utente CA User Activity Reporting Module per l'accesso ODBC o JDBC 705
Configurazione delle impostazioni del servizio ODBC 705
Creazione di un'origine dati ODBC "elm" 706
Modifica del file di configurazione di Crystal Reports 709
Esempio di creazione eventi per ODBC 711
Utilizzare Crystal Reports per accedere all'Archivio di registro eventi con ODBC 711
Accesso a Eventi da Crystal Reports con JDBC 713
Copiare i file JAR del driver JDBC 713
Utilizzare Crystal Reports per accedere all'Archivio registro eventi con JDBC 714
Eliminare il client ODBC sui sistemi Windows 715
Rimozione del client JDBC 715

Glossario **717**

Indice **749**

Capitolo 1: Introduzione

Questa sezione contiene i seguenti argomenti:

Informazioni sulla Guida (a pagina 19)

Informazioni sulla Guida

Questa *Guida all'amministrazione di CA Enterprise Log Manager* è dedicata alle attività successive all'installazione di CA User Activity Reporting Module e alla configurazione iniziale del server eseguite dall'amministratore. Alcune di queste attività vengono eseguite per apportare modifiche non frequenti al sistema, altre sono attività di routine eseguite in base a una pianificazione, altre ancora sono attività di monitoraggio continue.

Questa guida è dedicata a tutti i tipi di utente, compresi i seguenti:

- Gli amministratori che mantengono la configurazione del prodotto e gestiscono l'archiviazione dei log e gli aggiornamenti di sottoscrizione
- Gli analisti che utilizzano i rapporti per monitorare l'ambiente, creare rapporti personalizzati e pianificare la generazione degli avvisi
- I revisori che pianificano i rapporti, utilizzano query e rapporti per verificare la conformità agli standard e inseriscono annotazioni nei rapporti

Questa guida comprende un glossario dei termini ed un indice. Segue un sommario dei contenuti:

Sezione	Descrive le modalità per
Account utente	Configurare gli account utente con ruoli predefiniti e amministrarli autonomamente.
Criteri	Pianificare ruoli personalizzati e i criteri associati sulla base di ruoli e criteri predefiniti.
Ruoli e criteri predefiniti	Limitare l'accesso agli utenti con ruoli personalizzati, criteri personalizzati e filtri di accesso.
Servizi e adapter CA	Configurare il deposito eventi di log, il server di rapporto, il servizio di sottoscrizione e alcuni adattatori.
Archiviazione dei registri	Configurare l'archiviazione automatica e ripristinare i database archiviati.

Sezione	Descrive le modalità per
Sottoscrizione	Mantenere la configurazione di sottoscrizione, applicare aggiornamenti e ripristinare un backup di sottoscrizione
Filtri e profili	Limitare i dati visualizzati in un singolo rapporto o query o in tutti i rapporti e le query con filtri. Limitare l'elenco di tag, query e rapporti con i profili.
Query e rapporti	Creare, modificare e importare o esportare query e rapporti per visualizzare i log eventi attuali e recenti.
Avvisi	Creare un avviso per notificare gli utenti o le destinazioni di trap SNMP, oppure per eseguire un processo CA IT PAM al verificarsi di determinati eventi
Rapporti pianificati	Pianificare e mantenere i processi di rapporto, visualizzare ed annotare i rapporti generati
Soppressione e riepilogo	Creare e utilizzare regole di soppressione e aggregazione per ridurre il carico dei server e impedire la raccolta o l'elaborazione di eventi non desiderati.
Mapping e arsing	Creare ed utilizzare regole di mapping e parsing per perfezionare gli eventi non elaborati in vari formati, ottenendo valori standardizzati compatibili con la CEG, e per creare regole di inoltro eventi
Integrazioni e connettori	Creare integrazioni prodotto che, quando distribuite come connettori, consentono di perfezionare e trasmettere eventi da una singola origine evento al server CA User Activity Reporting Module.
Correlazione eventi e Gestione incidenti	Creare regole di correlazione evento in grado di riconoscere modelli di evento, denominati incidenti. Unire, modificare ed eliminare incidenti in base alla necessità.
Profili di raccolta evento	Creare profili di raccolta per la distribuzione della raccolta eventi in ambienti virtuali utilizzando l'API virtuale.
Agenti	Pianificare l'utilizzo di agenti, prepararne l'installazione, configurare agenti e gruppi di agenti ed applicare agli agenti aggiornamenti di sottoscrizione
Certificati personalizzati	Implementare certificati personalizzati per sostituire quelli predefiniti.
Funzioni di accessibilità	Utilizzare i controlli di accessibilità.

Sezione	Descrive le modalità per
Accedere agli eventi raccolti con ODBC/JDBC	Configurare rapporti personalizzati con un'utilità di creazione rapporti di terze parti, oppure recuperare le informazioni di log selezionate utilizzando prodotti di terze parti

Nota: per informazioni sul supporto del sistema operativo o sui requisiti di sistema, consultare le *Note della versione*. Per un tutorial sulla configurazione di un singolo sistema per la visualizzazione dei risultati delle query sugli eventi syslog e di Windows raccolti, consultare la *Guida generale.* Per informazioni dettagliate sulle procedure di installazione di CA User Activity Reporting Module e sull'esecuzione di una configurazione iniziale, consultare la *Guida all'implementazione.* Per ulteriori dettagli sull'installazione degli agenti, consultare la *Guida all'installazione degli agenti*. Per assistenza sull'utilizzo di una pagina di CA User Activity Reporting Module, consultare la Guida in linea.

Capitolo 2: Account utente

Questa sezione contiene i seguenti argomenti:

Attività di auto-amministrazione (a pagina 23)
Attività associate ai ruoli (a pagina 25)
Configurazione degli account con impostazioni predefinite (a pagina 37)
Creazione di un gruppo globale (a pagina 38)
Creazione di un utente globale (a pagina 39)
Assegnazione di un ruolo a un utente globale (a pagina 40)
Modalità di gestione degli account utente di riferimento (a pagina 42)
Linee guida per l'attivazione di un utente (a pagina 42)
Modifica di un account utente (a pagina 43)
Ripristino di una password utente (a pagina 45)
Eliminazione di un account utente (a pagina 46)

Attività di auto-amministrazione

Gli utenti con accesso a CA User Activity Reporting Module possono modificare le proprie password e sbloccare un account utente bloccato se l'archivio utente configurato è quello predefinito, ovvero l'archivio utente CA User Activity Reporting Module.

Quando l'amministratore crea un nuovo account utente, viene assegnata una nuova password. L'utente modifica tale password durante la prima sessione di accesso con una nuova che sia conforme ai relativi criteri che stabiliscono se è permessa una password corrispondente al nome utente, la lunghezza massima e minima, il numero massimo di caratteri ripetibili e il numero minimo di caratteri numerici. È responsabilità dell'utente modificare le password entro l'intervallo di frequenza specificato dai criteri delle password relativi alla durata massima e minima della stessa.

Gli utenti individuali amministrano i propri account come segue:

- Modificando le password in modo coerente con i criteri
- Sbloccando gli account utente che sono stati bloccati, se questo è permesso dal relativo criterio delle password.

Ulteriori informazioni:

Sblocco di un account utente (a pagina 24)
Modificare la propria password (a pagina 25)

Sblocco di un account utente

È possibile sbloccare un account utente bloccato a prescindere dal proprio ruolo, se il criterio di password lo prevede. Se l'account viene bloccato, dovrà essere sbloccato da un altro utente in modo che l'utente corrente possa accedere ai privilegi concessi al proprio ruolo.

Il blocco e lo sblocco sono controllati tramite i due criteri di password seguenti:

- Blocco dell'account utente dopo <n> accessi falliti.
- Consentire agli utenti di sbloccare le password.

È possibile che gi account utenti vengano bloccati se il criterio di password è impostato sul bloccaggio degli account a seguito del superamento di un numero prestabilito di tentativi non riusciti oppure se l'utente supera il numero consentito di tentativi di accesso con credenziali non valide.

Qualsiasi utente può sbloccare l'account di un altro utente se è stato impostato il criterio per consentire agli utenti di sbloccare le password. Per sbloccare l'account utente occorre la password dell'utente.

Per sbloccare un account utente

1. Fare clic sulla scheda Amministrazione e sulla sottoscheda Gestione utenti e accessi.
2. Fare clic sull'opzione Sblocca utente nel riquadro sinistro.
3. Immettere il nome utente e la password, quindi fare clic su Sblocca.

   L'account utente viene sbloccato.

Modificare la propria password

Indipendentemente dal tipo di ruolo, è possibile modificare la password. Se il criterio di password che definisce la validità massima della password è impostato, sarà necessario modificare la password con una frequenza adeguata al criterio.

Assicurarsi di modificare la password il più presto possibile nei seguenti casi:

- Se si comunica a qualcuno la propria password allo scopo di sbloccare l'account
- Se si dimentica la propria password e l'amministratore la reimposta

Per modificare la propria password

1. Fare clic sulla scheda Amministrazione e sulla sottoscheda Gestione utenti e accessi.
2. Fare clic su Modifica password nel riquadro sinistro.
3. Immettere la vecchia password.
4. Immettere la nuova password due volte.
5. Fare clic su OK.

Attività associate ai ruoli

Gli amministratori assegnano i ruoli agli utenti in base alle attività che dovranno eseguire. È possibile assegnare agli utenti il ruolo predefinito di revisore, analista e amministratore o personalizzare i ruoli creati. Per valutare l'impatto dell'utilizzo di ruoli predefiniti, rivedere le attività associate ad ogni ruolo.

Ulteriori informazioni:

Operazioni del revisore (a pagina 26)
Attività dell'analista (a pagina 28)
Attività dell'amministratore (a pagina 29)

Operazioni del revisore

I revisori interni possono eseguire le seguenti attività:

- Ricerca e selezione di una query e visualizzazione dei risultati
- Per una riga di risultati di query selezionata, eseguire un processo di output di evento/avviso configurato in CA IT PAM
- Visualizzazione dei rapporti correnti
- Pianificazione dei rapporti
- Visualizzazione dell'elenco dei processi di rapporto pianificati
- Visualizzazione dell'elenco dei rapporti generati
- Visualizzare ed annotare i rapporti generati
- Impostare filtri e profili

È possibile assegnare il ruolo di revisore con privilegi ridotti al momento della creazione degli account utente per il personale di terze parti. Ad esempio, quando un avviso pianificato esegue un processo di output di evento/avviso a livello di query, l'avviso invierà un URL a CA User Activity Reporting Module che verrà aggiunto alla descrizione. Per consentire al personale di terze parti di esplorare CA User Activity Reporting Module, è necessario fornire degli account utente.

Nota: analisti e amministratori possono eseguire tutte le attività del revisore, oltre a quelle specifiche del ruolo ricoperto.

I revisori esterni con accesso temporaneo a CA User Activity Reporting Module per il periodo della revisione possono verificare la conformità rispetto agli standard nelle seguenti aree:

- Verificare che i registri vengano raccolti dalle risorse previste.
- Verificare che esistano procedure per impedire la perdita dei dati. Ad esempio, verificare che il backup dei dati venga eseguito abbastanza frequentemente perché nulla venga perso.
- Verificare che i registri vengano controllati regolarmente per individuare violazioni della protezione.
- Verificare che i registri siano correttamente archiviati in un archivio protetto.
- Verificare che l'età dei dati archiviati soddisfi gli standard per la conservazione dei registri.

- Verificare che il contenuto dei registri includa i contenuti destinati alla memorizzazione.

Ulteriori informazioni:

Visualizzazione di un rapporto generato (a pagina 497)
Annotazioni a un rapporto generato (a pagina 499)
Visualizzazione di un rapporto (a pagina 279)
Esempio: eseguire un processo di output di evento/avviso con i risultati della query selezionata (a pagina 409)
Esempio: inviare un avviso che esegua un processo di IT PAM per query (a pagina 420)

Attività dell'analista

Gli analisti di sistema controllano la rete di raccolta dei log, per poi raccogliere e distribuire i dati di rapporto.

Gli amministratori assegnano il *ruolo di analista* agli utenti responsabili delle attività seguenti:

- Creazione e modifica di query e rapporti personalizzati

  Un rapporto è una visualizzazione grafica o tabulare dei dati del log eventi generata eseguendo query predefinite o personalizzate con filtri. I dati provengono da database hot, warm o defrosted dal deposito eventi di log del server selezionato e, se richiesto, dei server federati.

- Pianificazione degli avvisi

  Un avviso è un processo di query pianificato che è possibile utilizzare per individuare violazioni di criteri, tendenze di utilizzo, schemi di accesso e altre informazioni che richiedono attenzione a breve termine. I dati di avviso possono essere visualizzati nell'interfaccia utente oppure tramite feed RSS. È possibile inviare un avviso pianificato a destinatari di posta elettronica, ad una destinazione di trap SNMP oppure ad un processo CA IT PAM di output di evento/avviso. È possibile eseguire il processo una volta per riga oppure una volta per query.

- Creazione di tag

  Un *tag* è un termine o una frase chiave utilizzata per identificare query o rapporti appartenenti alla stessa categoria. Per aggiungere un nuovo rapporto ad un processo pianificato configurato per selezionare rapporti con uno specifico tag, aggiungere il tag comune al nuovo rapporto. Un tag può essere anche una frase chiave associata ad una query, che descrive il contenuto di quest'ultima e consente la classificazione e la ricerca in base alle frasi chiave.

- Visualizzazione dei feed RSS (Rich Site Summary)

  Un *evento RSS* è un evento generato da CA User Activity Reporting Module per convogliare un avviso verso prodotti ed utenti di terze parti. L'evento è un riepilogo del risultato di ogni avviso, ed un collegamento al file di risultato. È possibile configurare la durata di un dato elemento del feed RSS.

Gli analisti possono adottare il seguente approccio una volta acquisita familiarità con l'utilizzo di CA User Activity Reporting Module:

1. Esaminare i rapporti predefiniti disponibili. Anche i revisori possono eseguire questa operazione.
2. Progettare rapporti personalizzati, creare i relativi tag, pianificare, visualizzare, annotare.
3. Pianificare i rapporti da generare periodicamente. Anche i revisori possono eseguire questa operazione.
4. Rivedere i rapporti generati ed immettere le annotazioni. Anche i revisori possono eseguire questa operazione.
5. Identificare i criteri per l'invio di un avviso, il formato da utilizzare e il destinatario. Dopodichè, pianificare la generazione dell'avviso quando i criteri vengono soddisfatti.

Attività dell'amministratore

Gli utenti assegnati al ruolo di amministratore hanno accesso illimitato alle funzionalità disponibili da tutte le schede di CA User Activity Reporting Module. Solo gli utenti con ruolo di amministratore potranno disporre del completo accesso alla scheda Amministrazione. Dalla scheda Amministrazione, gli amministratori possono configurare e gestire tutti gli aspetti della raccolta di registri, oltre a tutti i servizi e gli accessi utente.

Ulteriori informazioni:

Configurazione e personalizzazione della raccolta di registri (a pagina 30)
Configurazione e monitoraggio dei servizi (a pagina 32)
Gestione utenti e accessi (a pagina 35)

Configurazione e personalizzazione della raccolta di registri

Solo gli utenti con ruolo di amministratore possono configurare e gestire le funzioni relative alla raccolta dei registri. Gli amministratori eseguono le attività di raccolta dei registri dalla sottoscheda Raccolta registri della scheda Amministrazione.

Gli amministratori utilizzano Explorer raccolta registri per configurare i connettori sugli agenti, operazione necessaria per la raccolta dei registri. Inoltre, gli amministratori applicano gli aggiornamenti di sottoscrizione agli agenti, quando è possibile.

È facoltativo utilizzare la libreria di perfezionamento eventi. Le funzionalità in dotazione, aggiornate regolarmente, sono pensate per soddisfare le esigenze della maggior parte dei clienti.

I processi dell'amministratore che coinvolgono la raccolta dei registri sono i seguenti:

- Configurare e gestire gli agenti installati da un server CA User Activity Reporting Module dedicato alla raccolta.
- Interrogare il catalogo archivio su un server di rapporto CA User Activity Reporting Module.

  Il *catalogo archivio* fornisce la registrazione di tutti i database esistiti sul server CA User Activity Reporting Module. Il catalogo di archivio comprende i database creati di recente, quelli che sono stati sottoposti a backup e spostati e quelli eventualmente eliminati prima del backup.
- Configurare gli adapter CA utilizzati da CA Audit.
- Informazioni sulla libreria di perfezionamento eventi.
  - Utilizzare le integrazioni predefinite e creare nuove integrazioni da zero o basandosi sulla copia di un'integrazione predefinita.

    L'integrazione consente di trasformare gli eventi non classificati in eventi perfezionati, in modo da poterli visualizzare nelle query e nei rapporti.
  - Creare un listener syslog dal listener predefinito.
  - Creare nuovi file di analisi da zero o basandosi su una copia del file predefinito selezionato.

    Un file di analisi dei messaggi (XMP), associato a uno tipo specifico di origine evento, consente di applicare regole di analisi che suddividono l'evento non elaborato in coppie nome/valore.

- Creare nuovi file di mapping da zero o basandosi su una copia del file predefinito selezionato.

  I file di mapping dei dati (DM) sono file XML che utilizzano la Grammatica evento comune (CEG) di CA per convertire gli eventi da un formato di origine a un formato che è possibile memorizzare nell'Archivio di registro eventi per l'analisi e la creazione di rapporti.

- Creare regole di riepilogo da zero o basandosi sulla copia di una regola predefinita selezionata.

  Le regole di riepilogo sono regole che uniscono alcuni eventi nativi di tipo comune ottenendo così un unico evento perfezionato.

- Creare regole di soppressione da zero o basandosi sulla copia di una regola predefinita selezionata.

  Le regole di soppressione impediscono la visualizzazione di certi eventi perfezionati nei rapporti.

- Creare regole di inoltro eventi.

  Le regole di inoltro eventi stabiliscono l'inoltro degli eventi selezionati a prodotti di terze parti, ad esempio prodotti che mettono in relazione gli eventi salvati nell'archivio di registro eventi.

- Creare profili.

  Un profilo specifica il gruppo di filtri dati e i tag visualizzati per la selezione. I filtri dati limitano i dati visualizzati in una query o in un rapporto. I filtri di tag limitano i tag visualizzati nell'elenco dei tag di query e di rapporto.

Ulteriori informazioni:

Modalità di creazione di un gruppo di agenti (a pagina 669)
Modalità di configurazione della gestione agente (a pagina 672)
Modalità di applicazione degli aggiornamenti di sottoscrizione (a pagina 679)

Configurazione e monitoraggio dei servizi

Solo gli utenti con il ruolo di amministratore possono configurare e gestire i servizi accessibili dalla scheda Amministrazione e dalla sottoscheda Servizi. Configurare tutti servizi subito dopo aver installato CA User Activity Reporting Module.

I processi di amministratore che comprendono servizi sono i seguenti:

- Configurare i seguenti servizi globali:
  - Intervallo di aggiornamento
  - Timeout di sessione
  - Se è necessaria l'autenticazione per visualizzare gli avvisi pubblicati sui feed RSS
  - Tag da nascondere
  - Profilo predefinito
- Configurare il servizio deposito eventi di log.
  - A livello globale, configurare i servizi che si applicano ai tutti i server di CA User Activity Reporting Module.
  - A livello locale, configurare l'archiviazione automatica.

    Il deposito eventi di log del server CA User Activity Reporting Module di raccolta ospita un database hot con nuovi registri. Il database hot viene compresso in un database warm quando raggiunge il numero massimo di righe configurato.

    - Se si configura l'archiviazione automatica tra il server di raccolta e quello di rapporto, il database warm verrà copiato sul server di rapporto e quindi eliminato dal server di raccolta.
    - Se si configura l'archiviazione automatica tra il server di rapporto e un server remoto che non è un server CA User Activity Reporting Module, i database warm vengono copiati sul server remoto su base oraria o giornaliera, a seconda delle impostazioni di archiviazione automatica. Per impostazione predefinita, il server di rapporto conserva i database fino a quando non raggiungono lo spazio su disco o i limiti di tempo impostati. I database vengono eliminati automaticamente dal server di rapporto solo se si seleziona la casella di controllo Server ELM remoto.

    - Se non si configura l'archiviazione automatica dal server di rapporto ad un server di archiviazione remota, creare manualmente un backup dei database warm e spostarli nell'archivio a lungo termine. Il database warm viene memorizzato nel deposito eventi di log di un server di rapporto (o di gestione/rapporto in una distribuzione a due server) per il numero di giorni di archiviazione massimo configurato, a meno che lo spazio disponibile sia inferiore alla percentuale configurata impostata per lo spazio sul disco di archiviazione. In questo caso, i database warm vengono eliminati a partire dal più datato.

- Configurare il servizio del server di rapporto.

  Il servizio del server di rapporto gestisce rapporti e avvisi, compresi criteri di ritenzione, il formato dei rapporti stampati ed inviati tramite posta elettronica e i valori con chiave di rapporti e avvisi. Inoltre, il servizio gestisce le impostazioni per l'integrazione dei processi CA IT PAM, ad esempio i processi di output di evento/avviso e di valori dinamici, nonché le impostazioni delle destinazioni di trap SNMP per gli avvisi.

- Configurare gli aggiornamenti di sottoscrizione.

  Gli aggiornamenti di sottoscrizione si riferiscono ai file binari e non binari resi disponibili dal server di sottoscrizione CA ai server CA User Activity Reporting Module, al componente CA EEM sul server di gestione e agli agenti.

- Gestire la federazione di server CA User Activity Reporting Module.

  È possibile impostare dal server di gestione una query da estendere ai figli della federazione e ai peer. I server CA User Activity Reporting Module possono essere federati per due scopi:

  - Il server di raccolta archivia automaticamente ogni database hot in un database warm e lo invia al relativo server di rapporto. Creare una federazione fra il server di raccolta e il server di rapporto. Quando si invia una query al server di gestione selezionando la federazione, è possibile ottenere risultati non solo dai database warm locali ma anche da quelli hot che si trovano sul server di raccolta.
  - È possibile creare più server di rapporto per distribuire l'archiviazione dei database warm tra più depositi eventi di log. È possibile federare i server di rapporto in un reticolo con ogni server di raccolta federato come figlio del corrispondente server di rapporto. Una query federata da ognuno dei server di rapporto a coppie restituisce dati da entrambi i server peer e da tutti i relativi server figli.

Nota: se si crea un punto di ripristino CA User Activity Reporting Module allo scopo di ripristinare i database archiviati dall'archiviazione a lungo termine, è consigliabile lasciare tale server al di fuori della federazione.

- Monitorare e gestire lo stato del sistema.

Ulteriori informazioni:

Backup e ripristino automatici (a pagina 191)
Invio di query al catalogo archiviazioni (a pagina 205)
Ripristino dei file archiviati automaticamente (a pagina 207)
Script per il ripristino di database archiviati (a pagina 208)
Considerazioni su ODBC Server (a pagina 165)
Creare un file di diagnostica di supporto (a pagina 181)
Riavviare un server host (a pagina 182)
Riavviare i servizi ELM. (a pagina 182)
Controllare lo stato e la versione dei servizi (a pagina 183)
Controllare gli eventi di automonitoraggio dello stato del sistema (a pagina 183)

Gestione utenti e accessi

Solo gli utenti con ruolo di amministratore possono configurare e gestire gli account utente, i criteri e gli altri oggetti di applicazione accessibili dalla sottoscheda Gestione utenti e accessi della scheda Amministrazione. Per accedere a CA User Activity Reporting Module, gli utenti devono disporre di un account configurato con un ruolo e delle relative credenziali di accesso. Ruoli e criteri predefiniti consentono agli amministratori di configurare l'accesso da parte degli utenti definendone gli account. È facoltativo creare ruoli e criteri personalizzati.

Le attività di amministratore relative a utenti e accessi comprendono le seguenti:

- Definire nuovi utenti globali (se l'archivio utenti è quello predefinito, ovvero l'archivio utenti CA User Activity Reporting Module).

  Quando si aggiunge un nuovo utente, si crea un utente globale. Informazioni quali nome, città e numero di telefono sono considerate globali perché possono essere condivise. Un *utente globale* è l'informazione dell'account utente che esclude i dettagli specifici dell'applicazione.

- Recuperare gli utenti di riferimento (se l'archivio utente è di riferimento).

  I dettagli dell'utente globale vengono memorizzati nell'archivio utente configurato, che può essere una directory esterna.

- Assegnare gruppi applicazione (ruoli) predefiniti o personalizzati a utenti nuovi o di riferimento.

  I dettagli dell'applicazione vengono sempre memorizzati nel repository del server di gestione. Questi dettagli sono caricati in formato di sola lettura quando si configura un archivio utenti esterno.

- Modificare, eliminare e visualizzare gli account utente.

- Creare gruppi applicazione personalizzati (ruoli) e i criteri associati.

  La creazione dei ruoli utente inizia con la definizione di un nuovo gruppo di utenti dell'applicazione e con la successiva creazione di un criterio che definisce le azioni consentite su specifiche risorse. Un ruolo utente può essere un gruppo utente di un'applicazione predefinita o un gruppo applicazione definito dall'utente. Sono necessari ruoli utente personalizzati quando i gruppi applicazione predefiniti (amministratore, analista e revisore) non sono sufficientemente dettagliati per riflettere le assegnazioni del lavoro. I ruoli utente personalizzati richiedono criteri di accesso personalizzati e la modifica dei criteri predefiniti per poter inserire il nuovo ruolo.

- Modificare, eliminare e visualizzare i gruppi di applicazioni ed i criteri associati.
- Modificare il criterio di accesso all'applicazione CALM.

  Il criterio di accesso all'applicazione CALM è un tipo di elenco di controllo di accesso del criterio di scoping che definisce chi può accedere a CA User Activity Reporting Module. Per impostazione predefinita, l'accesso è garantito all'amministratore [di gruppo], all'analista [di gruppo] e al revisore [di gruppo].
- Creare, modificare, eliminare e visualizzare i criteri di accesso.

  Un criterio di accesso è una regola che conferisce o nega ad un'identità (utente o gruppo utente) i diritti di accesso ad una risorsa applicazione.
- Configurare, modificare, eliminare e visualizzare i filtri di accesso.

  Un filtro di accesso è un filtro che può essere impostato da un amministratore per controllare quali dati evento possano essere visualizzati dai gruppi e dagli utenti non amministrativi. Ad esempio, un filtro di accesso può ridurre i dati che alcune identità specifiche possono visualizzare in un rapporto. I filtri di accesso vengono convertiti automaticamente in criteri di obbligo.

Ulteriori informazioni:

Creazione di un gruppo globale (a pagina 38)
Creazione di un utente globale (a pagina 39)
Assegnazione di un ruolo a un utente globale (a pagina 40)
Eseguire il backup di tutti i criteri di accesso (a pagina 61)
Ripristino dei criteri di accesso (a pagina 65)
Configurazione di ruoli utente personalizzati e criteri di accesso (a pagina 84)
Aggiunta di un'identità a un criterio esistente (a pagina 90)
Creazione di un criterio di accesso a CALM (a pagina 91)
Creazione di un criterio per un gruppo utente dinamico (a pagina 101)
Creazione di un criterio basato su un criterio esistente (a pagina 98)
Creazione di un criterio di scoping (a pagina 94)
Creazione di un filtro di accesso (a pagina 103)
Creazione di un gruppo utente delle applicazioni (ruolo) (a pagina 87)
Come garantire l'accesso ruolo personalizzato a CA User Activity Reporting Module (a pagina 88)
Verifica di un nuovo criterio (a pagina 100)
Creazione di un calendario (a pagina 105)

Configurazione degli account con impostazioni predefinite

Durante la configurazione di un ambiente di testing temporaneo, è possibile configurare rapidamente la gestione degli utenti e degli accessi utilizzando le impostazioni predefinite per gli account utente e configurando solo i campi obbligatori. Per il completamento della configurazione minima con le impostazioni predefinite, creare gli account utente per gli utenti CA User Activity Reporting Module nel seguente modo:

- Se si utilizza l'archivio utente predefinito, creare un account con un nome utente, assegnare un gruppo applicazione predefinito (amministratore, analista, revisore) e una password temporanea.
- Se si fa riferimento a un archivio utente esterno, cercare l'utente globale per nome e assegnargli un ruolo predefinito (amministratore, analista, revisore) e una password temporanea.

Ulteriori informazioni:

Creazione di un utente globale (a pagina 39)
Assegnazione di un ruolo a un utente globale (a pagina 40)
Modalità di gestione degli account utente di riferimento (a pagina 42)

Creazione di un gruppo globale

La possibilità di creazione di un gruppo globale dipende dalla configurazione dell'archivio utente. Si consideri quanto segue:

- Se si utilizza l'archivio utente predefinito, l'attività di creazione di gruppi globali è facoltativa.
- Se si fa riferimento a un archivio utente esterno, i gruppi globali e gli account utente vengono caricati automaticamente nell'archivio utente predefinito. Se lo si desidera, è possibile creare criteri personalizzati per tali gruppi globali, ma non si possono creare nuovi gruppi globali.
- Se l'archivio utente di riferimento corrisponde a CA SiteMinder, è possibile utilizzare i gruppi globali definiti in questo prodotto CA, oppure creare nuovi gruppi sulla base delle appartenenze a gruppi esistenti.

Per creare un gruppo globale

1. Fare clic sulla scheda Amministrazione e quindi sulla sottoscheda Gestione utenti e accessi.
2. Fare clic su Gruppi nel riquadro sinistro.

   Vengono visualizzati i riquadri dei gruppi utente e di ricerca dei gruppi.
3. Fare clic sul pulsante corrispondente al nuovo gruppo globale posizionato al lato della cartella dei gruppi globali.

   Viene visualizzato il riquadro relativo al nuovo gruppo utente globale.
4. Immettere un nome e una descrizione (facoltativo).
5. Se si desidera che il gruppo globale contenga altri gruppi globali, eseguire le seguenti operazioni:
   a. Specificare i criteri di ricerca per visualizzare un gruppo e fare clic su Cerca.
   b. Spostare il gruppo che si desidera includere nell'elenco dei gruppi utenti globali selezionati.
   c. Ripetere l'operazione per tutti i gruppi che si desidera includere nell'elenco.
6. Fare clic su Salva.

   Viene visualizzata una finestra di conferma.

Ulteriori informazioni:

Pianificazione del ruolo utente (a pagina 83)

Creazione di un utente globale

È possibile creare nuovi utenti soltanto se l'archivio utente è configurato come archivio utente CA User Activity Reporting Module (predefinito). La creazione di nuovi account utenti è consentita soltanto agli amministratori.

Se si fa riferimento a un archivio utente esterno, gli account utente vengono caricati automaticamente nell'archivio utente predefinito come record di sola lettura. Per creare un nuovo utente è necessario utilizzare l'archivio utente esterno. Il nuovo record verrà poi caricato automaticamente.

Per poter utilizzare il prodotto CA User Activity Reporting Module, l'utente dovrà disporre di un account utente globale. Tale account dovrà essere attivo al momento dell'accesso. Gli account possono diventare inattivi se sospesi dall'amministratore, bloccati a causa di una violazione ai criteri di password, o disabilitati a causa della scadenza dell'account attivato.

Per creare un nuovo account utente globale

1. Fare clic sulla scheda Amministrazione e sulla sottoscheda Gestione utenti e accessi.
2. Fare clic sul pulsante Utenti.
3. Verificare che l'account che si prevede di creare non esista già. Selezionare Utenti globali e fare clic su Vai a. Se il nome non viene visualizzato nei risultati, continuare.
4. Fare clic sul pulsante Nuovo utente a sinistra della struttura Utenti.

   Viene visualizzata la pagina Nuovo utente.
5. Immettere il nome dell'utente nel campo Nome.
6. (Facoltativo) Assegnare un gruppo utenti dell'applicazione.
   a. Fare clic su Aggiungi dettagli utente applicazione.
   b. Selezionare uno o più gruppi utente disponibili e fare clic sul pulsante Sposta per trasferire la selezione nella casella Gruppi utente selezionati.

      Nota: se non si desidera eseguire l'operazione, è possibile modificare l'account di un utente globale in un secondo momento ed assegnare un gruppo utenti dell'applicazione.

7. Immettere le informazioni generali nei dettagli relativi all'utente globale.
8. (Facoltativo) Assegnare un gruppo utente globale.
9. Completare le informazioni di autenticazione:
   a. Per impostare un numero massimo di tentativi di accesso prima di bloccare l'account, immettere un numero nel campo corrispondente. La configurazione con conteggio pari a 0 indica che non viene posto alcun limite.
   b. Lasciare deselezionata la casella di controllo Ignora criteri password, a meno che si voglia consentire a questo utente di possedere una password non conforme ai criteri delle password.
   c. Ripetere la password nella casella Conferma password.
   d. Selezionare Modifica password all'accesso successivo per consentire all'utente di modificare la password.
   e. Lasciare deselezionato Sospeso quando si crea un nuovo account.
   f. Immettere una nuova password nei campi Nuova password e Conferma password.
   g. Se l'utente dispone di un accesso temporaneo, immettere un intervallo di date per l'attivazione e la disattivazione dell'account.
   h. Per posticipare l'attivazione dell'account utente, inserire la data di abilitazione dell'account.
10. Fare clic su Salva.
11. Fare clic su Chiudi.

Assegnazione di un ruolo a un utente globale

È possibile eseguire la ricerca di un account utente esistente ed assegnare il gruppo utenti dell'applicazione al ruolo che si desidera venga eseguito. Se si fa riferimento a un archivio utente esterno, la ricerca restituisce record globali caricati da quell'archivio utente. Se l'archivio utente configurato è quello di CA User Activity Reporting Module, la ricerca restituisce i record creati per gli utenti in CA User Activity Reporting Module.

La modifica degli account utenti è consentita soltanto agli amministratori.

Per assegnare un ruolo (o un gruppo utenti dell'applicazione) a un utente esistente

1. Fare clic sulla scheda Amministrazione e sulla sottoscheda Gestione utenti e accessi.
2. Fare clic su Utenti nel riquadro sinistro.

   Vengono visualizzati i riquadri Ricerca utenti e Utenti.
3. Selezionare Utenti globali, inserire un criterio di ricerca e fare clic su Vai a.

   Se si stanno cercando account utente caricati, il riquadro Utenti mostra il percorso e le etichette percorso rispecchiano la directory esterna di riferimento.

   Importante: Immettere sempre i criteri di ricerca in modo che non vengano visualizzate tutte le voci in un archivio utente esterno.
4. Selezionare un utente globale senza appartenenza ad alcun gruppo applicazione CA User Activity Reporting Module.

   Viene visualizzata la pagina utente con il nome della cartella, i dettagli sull'utente globale e, laddove applicabile, l'appartenenza al gruppo globale.
5. Fare clic su Aggiungi dettagli utente applicazione.

   Il riquadro dettagli utente "CAELM" si espande.
6. Selezionare il gruppo desiderato da Gruppi utente disponibili e fare clic sulla freccia a destra.

   Il gruppo selezionato viene visualizzato nella casella del gruppo utenti selezionato.
7. Fare clic su Salva.
8. Verificare che il gruppo sia stato aggiunto.
   a. Dal riquadro di ricerca degli utenti, fare clic su Dettagli dell'applicazione utente, quindi fare clic su Vai.
   b. Verificare che il nome del nuovo utente dell'applicazione venga visualizzato tra i risultati.
9. Fare clic su Chiudi.

Modalità di gestione degli account utente di riferimento

È possibile utilizzare le informazioni dell'account utente globale quando in caso di archivio utente esterno. Sebbene il record utente non possa essere aggiornato nell'archivio utente esterno da CA User Activity Reporting Module, è possibile specificare dettagli a livello dell'applicazione.

Si raccomandano i seguenti approcci alla gestione degli accessi per gli utenti con account memorizzati in un archivio utente esterno.

- Aggiunta di un gruppo utente dell'applicazione (o ruolo) predefinito all'account utente.
- Aggiunta del gruppo globale ai criteri predefiniti per concedere l'accesso all'utente desiderato.
- Creazione di ruoli personalizzati e criteri associati e aggiunta del ruolo personalizzato all'account utente.

Linee guida per l'attivazione di un utente

Per l'utilizzo delle funzioni di attivazione dell'account, attenersi alle seguenti linee guida:

- Quando si procede alla creazione simultanea di più account utente, è possibile utilizzare l'opzione Data di attivazione per specificare una data futura di attivazione di tutti gli account o solo di quelli selezionati. In tal modo è possibile organizzare l'implementazione dei propri diritti di accesso per coordinarli con gli eventuali corsi di formazione per i nuovi utenti.
- Quando vengono creati account temporanei per i revisori esterni, è possibile utilizzare le impostazioni della data di attivazione e di disattivazione per specificare un intervallo di tempo determinato.
- Nel caso in cui venga rilevato un comportamento sospetto da parte di un utente, è possibile contrassegnare immediatamente l'account corrispondente per impedire a tale utente di accedere ai server CA User Activity Reporting Module.
- Quando un utente abbandona l'azienda, è possibile eliminare il record utente corrispondente e contrassegnarlo con lo stato sospeso oppure specificare una data di scadenza per modificarne lo stato in disabilitato.

Ulteriori informazioni:

Creazione di un utente globale (a pagina 39)
Modifica di un account utente (a pagina 43)
Eliminazione di un account utente (a pagina 46)

Modifica di un account utente

Gli account utente possono essere creati ed eliminati solo dagli utenti con ruolo di Amministratore. È possibile cercare un utente e visualizzarne le informazioni account corrispondenti per:

- Assegnare un ruolo CA User Activity Reporting Module, ovvero l'appartenenza a un gruppo di applicazioni, a un utente globale per il quale le informazioni account sono state caricate da un archivio utente di riferimento
- Aggiornare i dettagli dell'utente globale per un account dell'archivio utente locale
- Sospendere l'account utente
- Reimpostare la password per un account utente nel caso in cui l'account risulti bloccato o la password sia stata dimenticata e il criterio di password non consenta agli utenti di sbloccare gli account utente
- Disattivare un account utente oppure reimpostare la durata dell'account abilitato.

Importante: Non modificare il campo di conteggio degli accessi incorretti presente nell'area di autenticazione. Il valore visualizzato in questo campo viene aggiornato dal sistema.

Per modificare un account utente

1. Fare clic sulla scheda Amministrazione e sulla sottoscheda Gestione utenti e accessi.
2. Fare clic su Utenti nel riquadro sinistro.

   Viene visualizzato il riquadro di ricerca degli utenti.

3. Specificare i criteri di ricerca nel riquadro di ricerca degli utenti nei seguenti modi:
   - Per aggiungere dettagli dell'applicazione per l'utente globale, selezionare Utenti globali, inserire i criteri di ricerca e fare clic su Vai.
   - Per modificare l'account di un utente con un ruolo CA User Activity Reporting Module esistente, selezionare l'opzione dei dettagli utente dell'applicazione, immettere i criteri di ricerca e fare clic su Vai.

   Nota: per i criteri di ricerca, utilizzare l'operatore LIKE quando si specifica un carattere jolly come valore e utilizzare EQUAL quando si specifica la stringa completa. Di seguito si riportano alcuni esempi:
   - Appartenenza al gruppo LIKE Rev*
   - Appartenenza al gruppo EQUALS Revisore

   I nomi degli utenti che corrispondono alla ricerca vengono visualizzati nel pannello Utenti.
4. Fare clic sul nome utente dell'account da modificare.

   L'account selezionato verrà visualizzato nel riquadro destro.
5. Per aggiungere un ruolo, fare clic su Aggiungi dettagli utente applicazione, selezionare il ruolo appropriato da Gruppi utente disponibili e spostarlo in Gruppi utente selezionati.
6. Per aggiornare i dettagli dell'utente globale, sostituire i dettagli esistenti con quelli nuovi nella sezione Dettagli utente globale.

   Nota: i dettagli possono essere aggiornati soltanto se si utilizza l'archivio utente predefinito.
7. Per aggiornare una configurazione di autenticazione, eseguire una delle operazioni seguenti:
   - Selezionare Ignora criteri password per escludere l'utente dai controlli eseguiti da tutti i criteri di password.
   - Selezionare Sospeso per impedire all' utente di accedere ai server CA User Activity Reporting Module.
   - Deselezionare Sospeso per attivare l' account e consentire l'accesso all'utente.

- Se il criterio di password non consente agli utenti di sbloccare le password e la password utente risulta bloccata, selezionare Reimposta password, immettere la nuova password due volte, e selezionare Modifica password al prossimo accesso.

  Nota: il valore del campo di conteggio degli accessi incorretti aumenta automaticamente nel caso di tentativi di accesso incorretti e viene reimpostato su 0 una volta eseguito l'accesso. Se il valore del campo raggiunge o supera il valore del criterio di password impostato (numero di accessi non riusciti) l'account utente viene bloccato.

- Impostare il periodo di abilitazione dell'account facendo clic sull'opzione della data di attivazione per impostare una data di inizio e selezionando l'opzione relativa alla data di disattivazione per impostare la data di fine. Gli utenti dispongono dell'accesso dall'inizio del giorno della data di inizio alla fine del giorno della data di fine. Per consentire l' accesso per un solo giorno, specificare la stessa data di inizio e di fine.

8. Fare clic su Salva.

   Gli aggiornamenti apportati all'account utente vengono salvati ed entrano in vigore.

Ripristino di una password utente

È possibile ripristinare la password di un utente, nel caso in cui sia stata dimenticata. Se l'utente ha dimenticato la password e l'accesso viene bloccato a causa del superamento del numero consentito di tentativi di accesso, è possibile reimpostare la password. In tal modo l'utente potrà sbloccare l'account, se i criteri password consentono questa operazione.

Per ripristinare una password utente:

1. Fare clic sulla scheda Amministrazione e sulla sottoscheda Gestione utenti e accessi.
2. Fare clic sul pulsante Utenti.
3. Cercare l'account utente da modificare.
   a. Fare clic su Dettagli utente applicazione.
   b. Inserire il nome utente nel campo Valore, dove Attributo è impostato su Nome utente e Operatore su LIKE.
   c. Fare clic su Vai.

4. Fare clic sul nome dell'utente nella struttura Utenti.

   Vengono visualizzati i dettagli dell'account utente selezionato.

5. Nel riquadro Autenticazione, selezionare Reimposta password.

   Vengono visualizzati i campi Nuova password e Conferma password.

6. Immettere la nuova password nei campi Nuova password e Conferma password.

7. Fare clic su Salva, quindi su Chiudi.

Eliminazione di un account utente

È possibile eliminare qualsiasi account utente globale creato in CA User Activity Reporting Module.

Per disattivare un account utente senza eseguirne l'eliminazione, procedere in uno dei seguenti modi:

- È possibile impostare una data di disattivazione per l'account.
- È possibile sospendere un account per impedire l'accesso all'interfaccia CA User Activity Reporting Module da parte dell'utente associato.

Per eliminare un utente globale

1. Fare clic sulla scheda Amministrazione, la sottoscheda Gestione utenti e accessi e il pulsante Utenti.

   Vengono visualizzati i riquadri Ricerca utenti e Utenti.

2. Selezionare Utenti globali o Dettagli utente applicazione, specificare i criteri di ricerca e fare clic su Vai a.

3. Selezionare l'utente da eliminare dall'elenco degli utenti esistenti.

   Il record dell'utente selezionato viene visualizzato nel riquadro destro.

4. Fare clic su Elimina.

   Viene visualizzato un messaggio di conferma per l'eliminazione di questo utente.

5. Fare clic su OK.

   Viene visualizzato il messaggio di conferma "Utente globale eliminato correttamente".

   Nota: se si seleziona nuovamente Vai nel riquadro Cerca utenti, l'elenco visualizzato non contiene il nome dell'utente specificato.

Capitolo 3: Criteri

Per creare ruoli personalizzati è necessaria la modifica dei criteri predefiniti e la creazione di criteri personalizzati. Prima di eseguire tali attività, si consiglia di esaminare i criteri predefiniti associati a ciascun ruolo predefinito. È consigliabile sottoporre a backup i criteri di accesso predefiniti prima di apportare qualsiasi modifica.

Questa sezione contiene i seguenti argomenti:

Introduzione ai criteri (a pagina 48)
Criteri di accesso predefiniti (a pagina 48)
Eseguire il backup di tutti i criteri di accesso (a pagina 61)
Ripristino dei criteri di accesso (a pagina 65)

Introduzione ai criteri

Un *criterio di accesso* è una regola che conferisce o nega ad un'identità, quale un utente o un gruppo di utenti, i diritti di accesso ad una risorsa globale o di applicazione. CA User Activity Reporting Module stabilisce se i criteri siano applicabili ad un utente specifico facendo corrispondere identità, risorse e classi di risorse, e valutando i filtri. In altre parole, un criterio specifica le azioni consentite o negate ad identità specifiche riguardo specifiche risorse. I criteri che negano l'accesso a una data risorsa hanno la precedenza su quelli che ne garantiscono l'accesso.

CA User Activity Reporting Module supporta le seguenti tipologie di criteri di accesso:

- Criteri di accesso CALM
- Criteri di delega
- Criteri gruppo utente dinamici (un approccio alternativo ai gruppi applicazione personalizzati)
- Criteri di obbligo (creati automaticamente quando si costruisce un filtro di accesso)
- Criteri di scoping

CA User Activity Reporting Module viene installato con criteri CALM di accesso e di scoping predefiniti per tre gruppi utente dell'applicazione CA User Activity Reporting Module, ovvero amministratore, analista e revisore. Questi criteri sono sufficienti se si prevede di assegnare agli utenti che operano nei vari ruoli solo i gruppi utente forniti dall'applicazione.

Importante: Si consiglia di eseguire un backup dei criteri predefiniti disponibili in CA User Activity Reporting Module. Se si elimina inavvertitamente un criterio di accesso di CALM, gli utenti non potranno accedere a CA User Activity Reporting Module finché tale criterio non sarà ripristinato da un backup.

Criteri di accesso predefiniti

Se si utilizzano solo le funzioni in dotazione, assegnando un gruppo applicazione predefinito (amministratore, analista o revisore) come ruolo per ogni utente, non occorre creare alcun criterio di accesso. Tutti criteri necessari sono predefiniti e pronti per l'utilizzo.

Ulteriori informazioni:

Esaminare i criteri per tutti gli utenti. (a pagina 49)
Esaminare i criteri per i revisori (a pagina 53)
Esaminare i criteri per gli analisti (a pagina 55)
Esaminare i criteri per gli amministratori (a pagina 58)
Risorse ed azioni (a pagina 76)

Esaminare i criteri per tutti gli utenti.

È possibile esaminare i criteri per tutti gli utenti. Modificare il Criterio di accesso all'applicazione di CALM per definire ruoli personalizzati. A questo criterio si devono aggiungere come identità tutti i ruoli personalizzati.

Per esaminare i criteri per tutti gli utenti

1. Fare clic sulla scheda Amministrazione e quindi sulla sottoscheda Gestione utenti e accessi.
2. Fare clic su Criteri di accesso nel riquadro a sinistra.
3. Visualizzare il Criterio di accesso all'applicazione CALM come segue:
   a. Selezionare Mostra criteri di nome corrispondente.
   b. Digitare CALM*.
   c. Fare clic su Vai.
4. Esaminare il Criterio di accesso all'applicazione CALM.

   Tale criterio assegna l'accesso in lettura e in scrittura alle risorse elencate per tutti i membri dei gruppi di utenti dell'applicazione predefiniti (amministratore, analista e revisore) e a quelli che utilizzano l'API di CA User Activity Reporting Module:

Criteri di accesso

<< < 1 / 1 > >>

Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	Concessione esplicita	ug:Administrator ug:Analyst ug:Auditor CALM_API_UT	read write	ApplicationInstance AppObject Policy User GlobalUser

Le descrizioni elencate sono le seguenti:

- La risorsa ApplicationInstance è CAELM, che si riferisce al prodotto CA User Activity Reporting Module.
- Criterio si riferisce ai criteri di accesso.
- Utente è un qualsiasi utente aggiunto ad un gruppo di utenti dell'applicazione di CA User Activity Reporting Module.
- GlobalUser è un qualsiasi utente definito nell'archivio utente in CA User Activity Reporting Module, o ad esso riferito da CA User Activity Reporting Module.
- AppObject, con il valore pozFolder nella cartella Profili, fa riferimento ai profili.
- AppObject con il valore pozFolder nella cartella flex si riferisce all'XML con intervallo di tempo dinamico utilizzato per compilare l'elenco a discesa degli intervalli nel passaggio Condizioni risultato delle procedure guidate basate su query.

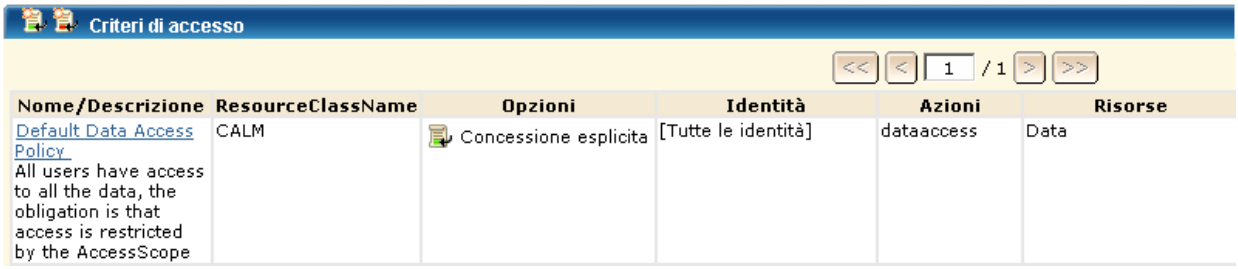
Il filtro per l'accesso all'applicazione CALM indica le limitazioni di azione su ogni risorsa.

Filtri					
DOVE	(	req:resource	==	val:ApplicationInstance	
E		req:action	{}	val:read	)
O	(	req:resource	==	val:Policy	
E		req:action	{}	val:read	)
O	(	req:resource	==	val:User	
E		req:action	{}	val:read,write	
E		name:cn	==	req:identity	)
O	(	req:resource	==	val:GlobalUser	
E		req:action	{}	val:read	
E		name:cn	==	req:identity	)
O	(	req:resource	==	val:AppObject	
E		req:action	==	val:read	
E		name:pozFolder	*--*	val:/CALM_Configuration/Content/Profiles	)

5. Ricercare i criteri per tutti gli utenti come segue:
   a. Fare clic su Criteri di accesso nel riquadro a sinistra.
   b. Selezionare Mostra criteri di identità corrispondente. Eliminare le altre selezioni.
   c. Inserire [Tutte le identità] nel campo Aggiungi identità.
   d. Fare clic su Aggiungi.
   e. Fare clic su Vai.

   Verranno visualizzati quattro criteri, compresi il criterio CEG e quello Predefinito di accesso ai dati (se non si inserisce esplicitamente [Tutte le identità], verranno visualizzati molti altri criteri aggiuntivi).
6. Esaminare il Criterio predefinito di accesso ai dati.

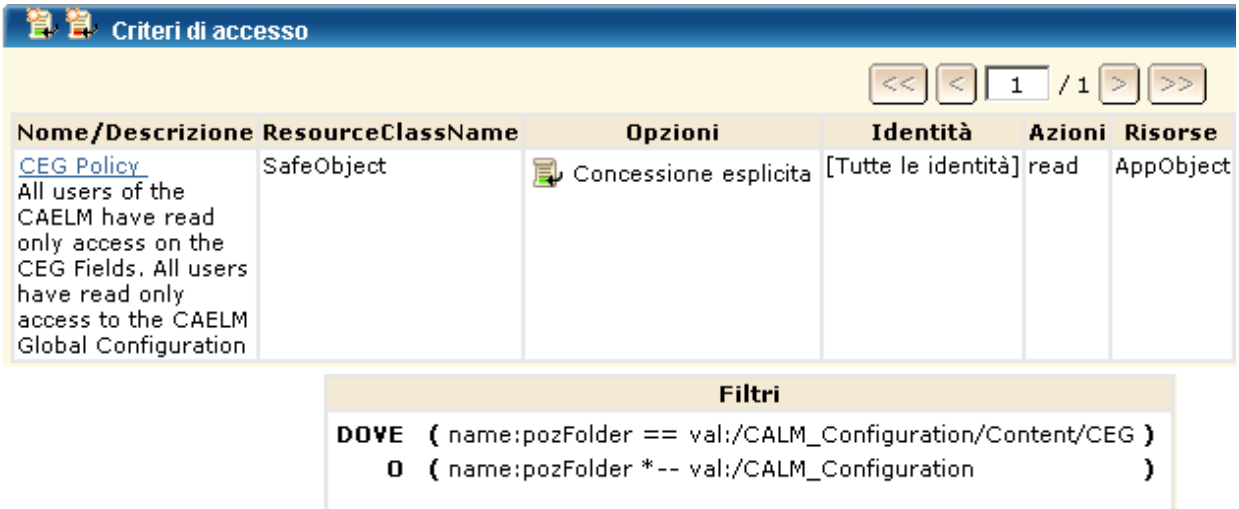
   Il Criterio predefinito di accesso ai dati nella classe di risorsa di CALM assegna a tutti gli utenti l'accesso ai dati di CA User Activity Reporting Module al livello specificato in un filtro di accesso. Un filtro di accesso si traduce in un criterio di obbligo con l'azione FulfillOnGrant su dataaccess/CALM/Data.



Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
Default Data Access Policy All users have access to all the data, the obligation is that access is restricted by the AccessScope	CALM	Concessione esplicita	[Tutte le identità]	dataaccess	Data

7. Esaminare il criterio di scoping Criterio CEG.

   Il Criterio CEG predefinito garantisce a tutti gli utenti con Accesso alle applicazioni CALM la possibilità di visualizzare i campi di Grammatica evento comune. Pertanto, i campi CEG verranno visualizzati negli elenchi a discesa per i filtri semplici ed avanzati di tutti gli utenti, poiché tutti gli utenti possono impostare filtri globali e locali per le query da essi eseguite. Gli utenti con diritti sufficienti per creare e modificare le query possono impostare i filtri per le query da loro create e modificate. Questo criterio assicura che tutti gli utenti possano visualizzare le impostazioni di Configurazione globale.



Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
CEG Policy All users of the CAELM have read only access on the CEG Fields. All users have read only access to the CAELM Global Configuration	SafeObject	Concessione esplicita	[Tutte le identità]	read	AppObject

Filtri	
DOVE	(name:pozFolder == val:/CALM_Configuration/Content/CEG)
O	(name:pozFolder *-- val:/CALM_Configuration)

Esaminare i criteri per i revisori

È possibile esaminare i criteri predefiniti per i revisori in modo da capire in che modo essi limitano l'accesso da parte delle applicazioni alle risorse necessarie per eseguire le seguenti operazioni.

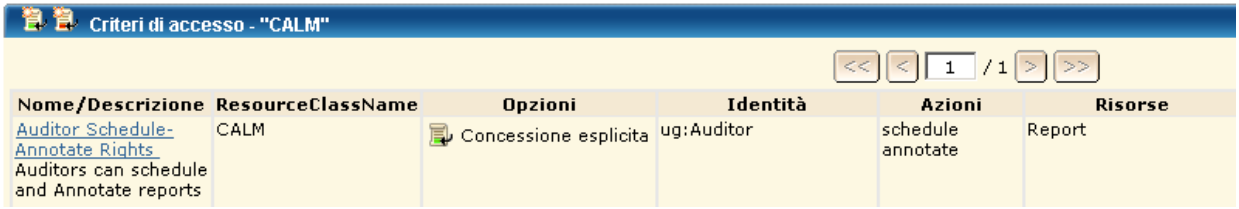
- Pianificare ed annotare i rapporti
- Visualizzare i rapporti.

Per esaminare i criteri predefiniti per i revisori

1. Fare clic sulla scheda Amministrazione e sulla sottoscheda Gestione utenti e accessi.
2. Fare clic su Criteri di accesso nel riquadro a sinistra.
3. Cercare i criteri per i revisori come segue:
   a. Selezionare Mostra criteri di identità corrispondente.
   b. Inserire ug:Auditor nel campo Aggiungi identità.
   c. Fare clic su Aggiungi.
   d. Fare clic su Vai.

   Verranno visualizzati tutti i criteri per [Tutte le identità] e ug:Auditor.
4. Esaminare il criterio Pianificare revisore-Annotare diritti.

   Tutti i criteri di accesso a CALM definiscono le azioni che è possibile eseguire nei confronti delle risorse specifiche di applicazioni. Tale criterio conferisce agli utenti assegnati al gruppo utente dell'applicazione Revisore la possibilità di pianificare ed annotare i rapporti.

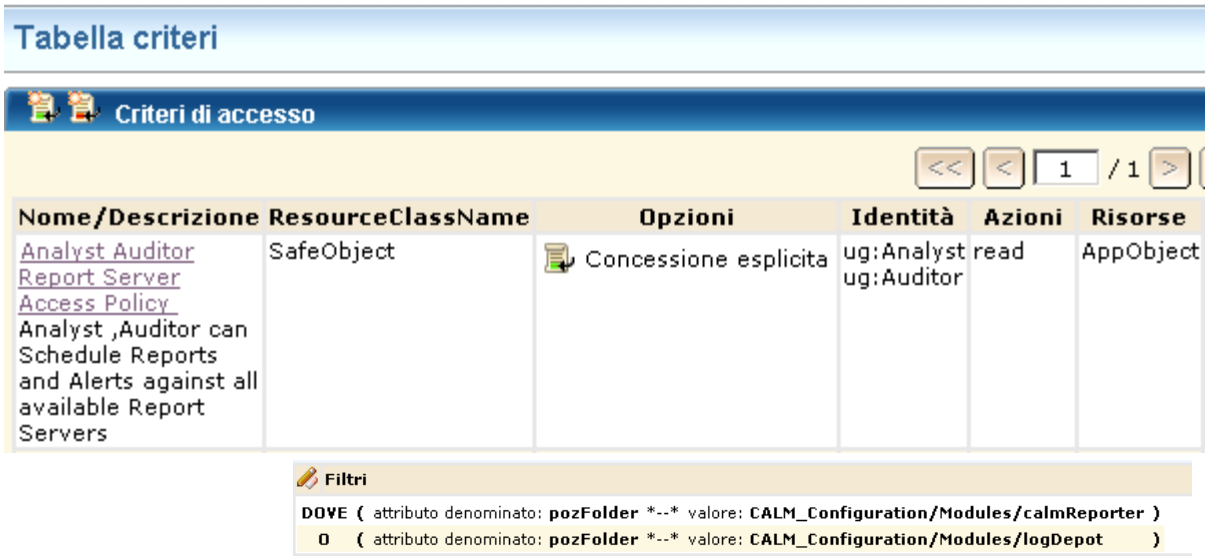


Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
Auditor Schedule-Annotate Rights Auditors can schedule and Annotate reports	CALM	Concessione esplicita	ug:Auditor	schedule annotate	Report

Confrontare questo criterio con il Criterio di creazione-pianificazione-annotazione per analisti e con il Criterio di creazione per l'amministratore.

5. Esaminare il Criterio di accesso al server di rapporto per analisti e revisori.

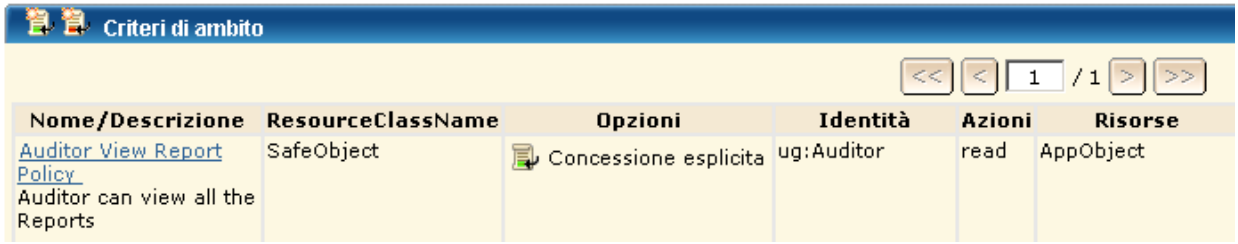
   Questo criterio di scoping consente ai revisori di impostare la destinazione dei rapporti in qualunque server di rapporto e di creare un rapporto federato che richiede l'accesso ad ogni Archivio registro eventi. La risorsa elencata nel criterio è AppObject, in cui gli oggetti applicazione sono Server di rapporto ed Archivi registro eventi.



   Nota: per un dato criterio di accesso di CALM, ovvero un criterio per la classe di risorsa di CALM, esiste di solito un criterio di scoping correlato per la classe di risorsa SafeObject.

6. Esaminare il criterio Revisore visualizza rapporto.

   Tale criterio di scoping garantisce agli utenti l'accesso in lettura ai rapporti. La risorsa elencata nel criterio è AppObject.



   AppObject è limitato a specifiche risorse applicazione con un filtro che garantisce il diritto di visualizzare i rapporti. Il percorso è quello della cartella EEM in cui risiedono i contenuti di tutti rapporti.

Esaminare i criteri per gli analisti

È possibile esaminare i criteri predefiniti per gli analisti in modo da vedere come essi limitano l'accesso delle applicazioni alle risorse necessarie per eseguire le seguenti operazioni:

- Pianificare ed annotare i rapporti (operazioni del revisore)
- Visualizzare i rapporti (operazione del revisore)
- Creare rapporti e tag
- Creare e pianificare gli avvisi (query)
- Modificare rapporti, avvisi e tag

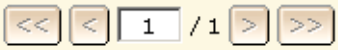
Per esaminare i criteri predefiniti per gli analisti

1. Fare clic sulla scheda Amministrazione e sulla sottoscheda Gestione utenti e accessi.
2. Fare clic su Criteri di accesso nel riquadro a sinistra.
3. Cercare i criteri per gli analisti come segue:
   a. Deselezionare Mostra criteri di nome corrispondente.
   b. Selezionare Mostra criteri di identità corrispondente.
   c. Inserire ug:Analyst nel campo Aggiungi identità.
   d. Fare clic su Aggiungi.
   e. Fare clic su Vai.
4. Verranno visualizzati tutti i criteri per ug:Analyst, compresi quelli per [Tutte le identità] che contengono questo gruppo di utenti.

5. Esaminare il Criterio di creazione-pianificazione-annotazione per analisti.

   Questo criterio di accesso a CALM definisce le azioni che possono essere eseguite nei confronti di specifiche risorse applicazione. Il criterio conferisce agli utenti assegnati al gruppo di utenti dell'applicazione di CA User Activity Reporting Module denominato Analista la possibilità di creare, pianificare ed annotare i rapporti, creare e pianificare gli avvisi e creare tag. (i revisori possono solo pianificare ed annotare i rapporti).

Criteri di accesso



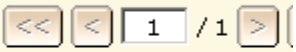
Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
Analyst Create-Schedule-Annotate policy Analyst can create/schedule Reports, create profiles, schedule Action Alerts,Annotate Reports	CALM	Concessione esplicita	ug:Analyst	create schedule annotate	Report Alert Tag Profile

6. Esaminare il Criterio di accesso al server di rapporto per analisti e revisori.

   Questo criterio di scoping consente agli analisti di pianificare i diritti per ogni server di rapporto. La risorsa elencata nel criterio è AppObject.

Tabella criteri

Criteri di accesso



Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
Analyst Auditor Report Server Access Policy Analyst ,Auditor can Schedule Reports and Alerts against all available Report Servers	SafeObject	Concessione esplicita	ug:Analyst ug:Auditor	read	AppObject

AppObject si limita alle specifiche risorse con filtri.

Filtri	
DOVE	(name:pozFolder *--* val:CALM_Configuration/Modules/calmReporter)
O	(name:pozFolder *--* val:CALM_Configuration/Modules/logDepot)

- Il filtro che termina in calmReporter garantisce l'accesso in lettura a tutti i server di rapporto. Una volta pianificato un rapporto, si specificheranno anche i server di rapporto di destinazione da cui saràn possibile visualizzare il rapporto generato.
- Il filtro che termina in logDepot garantisce l'accesso a tutti gli Archivi registro eventi. Quando si definisce un rapporto come federato, le query vengono eseguite sui dati in tutti gli archivi registro eventi idonei. L'idoneità dipende dalla posizione nella gerarchia del server in cui viene avviato il rapporto nelle federazioni gerarchiche.

7. Esaminare il Criterio di visualizzazione-modifica rapporti per analisti.

   Questo criterio di scoping conferisce agli utenti con ruolo di analista la possibilità di visualizzare, modificare o eliminare qualsiasi rapporto. La risorsa specificata nel criterio è AppObject.

Criteri di ambito

<< < 1 / 1 > >>

Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
Analyst Report View-Edit Policy Analyst can View/Edit any Report	SafeObject	Concessione esplicita	ug:Analyst	read write	AppObject

   AppObject si limita ai rapporti in base al seguente filtro, che conferisce il diritto di visualizzare i rapporti generati e salvati nella cartella EEM /CALM_Configuration/Content/Reports.

Filtri
DOVE (name:pozFolder *--* val:/CALM_Configuration/Content/Reports)

   Nota: la possibilità di modificare i rapporti conferita da questo criterio si può estendere in base al criterio CEG, che assegna il diritto di aggiungere filtri ai rapporti utilizzando le colonne CEG.

Esaminare i criteri per gli amministratori

Gli amministratori assegnano il ruolo di amministratore agli utenti che dovranno avere accesso completo all'applicazione CA User Activity Reporting Module e a tutte le sue funzioni. È possibile esaminare i criteri predefiniti per gli amministratori per capire come conferire l'accesso agli utenti che dovranno eseguire le seguenti operazioni:

- Creare EventGrouping, ovvero regole di soppressione e riepilogo utilizzando la grammatica evento comune.
- Creare Integration, ovvero file di mapping dei dati e analisi dei messaggi utilizzando la grammatica evento comune
- Creare EventForwarding, ovvero regole per l'inoltro degli eventi a sistemi di terze parti.
- Eseguire Database, ovvero la query con Query di catalogo archiviazioni per i nomi dei database sottoposti a backup e trasferiti in una soluzione di archiviazione esterna.
- Visualizzare o modificare i criteri.
- Visualizzare o modificare i calendari definiti dall'utente.
- Visualizzare o modificare un qualsiasi oggetto di applicazione. Gli oggetti di applicazione sono modelli di rapporto, modelli di query, processi di rapporto pianificati, processi di avviso, profili, delle configurazioni di servizio, file di mapping dei dati (DM), file di analisi dei messaggi (XMP), regole di soppressione e riepilogo e regole di inoltro eventi.
- Creare filtri con l'attributo iPoz di AppObject
- Visualizzare le cartelle elencate in Amministrazione, Gestione utenti e accessi, Cartelle EEM e modificare i dati definiti dall'utente in esse presenti.
- Visualizzare o modificare i dettagli di qualsiasi utente applicazione, gruppo utenti applicazione o utente globale.
- Qualsiasi attività di analista o revisore.

Per esaminare i criteri predefiniti per gli amministratori

1. Fare clic sulla scheda Amministrazione e quindi sulla sottoscheda Gestione utenti e accessi.
2. Fare clic su Criteri di accesso nel riquadro a sinistra.

3. Cercare i criteri per gli amministratori come segue:
   a. Selezionare Mostra criteri di identità corrispondente.
   b. Inserire ug:Adminstrator nel campo Aggiungi identità.
   c. Fare clic su Aggiungi.
   d. Fare clic su Vai.

   Verranno visualizzati tutti i criteri relativi a [Tutte le identità] e ug:Administrator.

4. Esaminare il criterio di accesso a CALM chiamato Criterio di creazione per l'amministratore.

   Questo criterio definisce le azioni che possono essere eseguite su specifiche risorse applicazione. Il criterio conferisce agli utenti assegnati al gruppo di utenti dell'applicazione, Amministratore, la possibilità di eseguire le azioni specificate applicabili alle risorse indicate.

Criteri di accesso

<< < 1 / 1 > >>

Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
Administrator Create policy Administrator can create any object	CALM	Concessione esplicita	ug:Administrator	create schedule annotate edit	Report Alert Profile Tag Integration EventGrouping EventForwarding Database

5. Esaminare il criterio di accesso a CALM chiamato Criterio amministratore gestione agente.

   Il criterio consente agli amministratori di creare gruppi di agenti, modificare tutti i gruppi di agenti, configurare i connettori e creare integrazioni. Il criterio consente agli amministratori di modificare la chiave di autenticazione dell'agente per l'istanza di applicazione del server CA User Activity Reporting Module in cui l'agente trasferisce gli eventi raccolti. Per impostazione predefinita, la Chiave di autenticazione agente configurata si applica a tutti i server CA User Activity Reporting Module attraverso tutte le istanze applicazione, ma è possibile impostarla in modo che sia univoca per l'istanza applicazione.

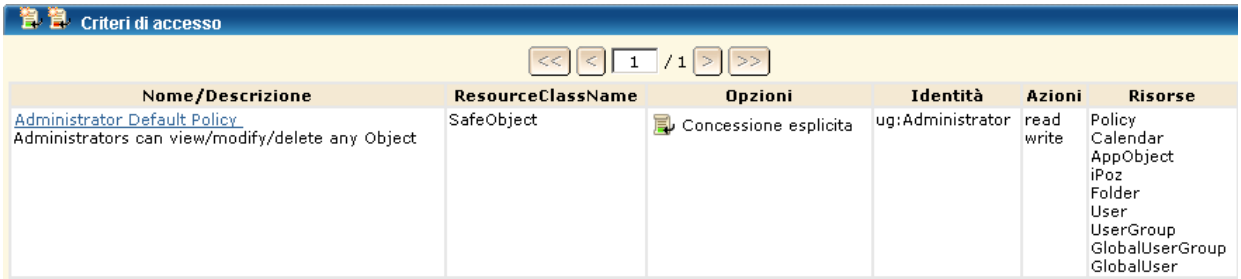
Criteri di accesso

<< < 1 / 1 > >>

Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
Admin Agent Manager Policy Access Rights for Admnistrator for Agent Management	CALM	Concessione esplicita	ug:Administrator	edit	AgentConfiguration AgentAuthenticationKey Connector ALL_GROUPS Integration

6. Esaminare il criterio di scoping chiamato Criterio predefinito amministratore.

   Tale criterio conferisce agli amministratori il diritto di visualizzare, modificare o eliminare le risorse elencate. Le risorse elencate non sono specifiche di CA User Activity Reporting Module e AppObject. AppObject si riferisce ad oggetti specifici dell'applicazione, che corrispondono alle risorse elencate nel Criterio di creazione per l'amministratore e nel Criterio amministratore gestione agente di CALM.



Criteri di accesso

<< < 1 / 1 > >>

Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
Administrator Default Policy Administrators can view/modify/delete any Object	SafeObject	Concessione esplicita	ug:Administrator	read write	Policy Calendar AppObject iPoz Folder User UserGroup GlobalUserGroup GlobalUser

Criteri di accesso per i prodotti registrati

Quando si registra un prodotto con CA User Activity Reporting Module, si genera un nuovo certificato per poi aggiornare alcuni criteri di accesso in modo da consentire l'accesso di sola lettura a tutti i tag, le query e i rapporti. Più precisamente, il nome certificato utilizzato per autenticare il prodotto registrato verrà aggiunto come nome di certificato Identità ai seguenti criteri:

- Accesso all'applicazione CALM
- Criterio di accesso al server di rapporto per analisti e revisori
- Criterio di visualizzazione-modifica rapporti per analisti

L'aggiunta del nome certificato ai criteri consente agli utenti di qualsiasi prodotto CA o di terze parti, o ad un cliente di CA, di ottenere un elenco delle query e dei rapporti in base al tag. Tali utenti possono visualizzare gli elenchi all'interno della propria interfaccia e recuperare i dati evento perfezionati necessari.

Eseguire il backup di tutti i criteri di accesso

L'esportazione dei criteri di accesso predefiniti è il metodo consigliato per conservare una copia di backup in caso di eliminazione o danneggiamento di un criterio di accesso.

Importante: Poiché il danneggiamento dei criteri può verificarsi durante il riavvio del sistema o del servizio CA EEM, è importante disporre di una copia di backup per il ripristino. Si consiglia inoltre di eseguire periodicamente il backup di CA EEM, ad esempio dopo l'installazione di un nuovo CA User Activity Reporting Module o dopo la creazione di criteri personalizzati.

È possibile esportare tutti i criteri per ogni tipo di criterio di accesso. Quando si esportano i criteri, viene creato un file XML per ogni criterio del tipo selezionato. I file XML vengono compressi in un file .zip denominato CAELM[1].xml.gz, contenente il documento CAELM[1].xml. Salvare il file .zip esportato in una directory a scelta.

Prima di poter ripristinare il file di backup salvato, è necessario copiarlo nella seguente directory di CA User Activity Reporting Module con l'archivio utente interno: /opt/CA/LogManager/EEM. Questa copia può essere realizzata dopo un salvataggio nella directory locale; altrimenti, si può aspettare e copiarla solo se è necessario un ripristino.

Il formato di esportazione dei criteri dipende dal numero di oggetti esportati.

- *filename*.tar.gz viene utilizzato se il numero di oggetti esportati è elevato.
- *filename*.xml.gz viene utilizzato per un numero di oggetti esportati ridotto o moderato.

Durante l'esportazione, si consiglia di rinominare *filename* (CAELM[n]) con un nome pertinente. Ad esempio, esportare i file dalle tre cartelle dei criteri contenenti criteri predefiniti con il nome CAELM_CriteriAccessoCalm, CAELM_CriteriEvento e CAELM_CriteriScoping.

Nota: deve essere mantenuta la stessa estensione, ovvero xml.gz o tar.gz.

È possibile estrarre il file XML contenente la definizione dei criteri di accesso dal file .zip ed utilizzarlo come input per l'utilità safex, utilizzata per il ripristino dei criteri di accesso.

Per eseguire il backup di tutti i criteri di accesso

1. Fare clic sulla scheda Amministrazione e quindi sulla sottoscheda Gestione utenti e accessi.
2. Eseguire il backup dei criteri di accesso CALM predefiniti attenendosi alla procedura riportata di seguito:
   a. Fare clic sul pulsante Criteri di accesso.
   b. Fare clic su CALM.

      Viene visualizzata la tabella di quel criterio, Criteri di accesso - CALM.
   c. Fare clic sul pulsante Esporta.
   d. Viene visualizzata la finestra di dialogo Download file, contenente le opzioni di apertura o salvataggio.
   e. (Facoltativo) Fare clic su Apri per aprire il file compresso CAELM[1].xml.gz. Fare doppio clic su CAELM[1].xml per esaminare il file in formato XML.
   f. Fare clic su Salva per salvare il file.

      Viene visualizzata la finestra di dialogo Salva con nome.
   g. Selezionare la cartella di destinazione, modificare il nome del file se desiderato, quindi fare clic su Salva.

      Se non si modifica il nome, il file .zip viene salvato come CAELM[1].xml.gz.
   h. Fare clic su Chiudi.

      La finestra di dialogo Download completato verrà chiusa. L'elenco dei criteri resta visualizzato nel riquadro a sinistra.

3. Eseguire il backup dei criteri evento predefiniti come segue:
   a. Fare clic su Criteri evento.

      Viene visualizzata la tabella Criteri evento
   b. Fare clic sul pulsante Esporta.
   c. Viene visualizzata la finestra di dialogo Download file, contenente le opzioni di apertura o salvataggio.
   d. Fare clic su Salva per salvare il file.

      Viene visualizzato un messaggio che chiede se si desidera sostituire il file CAELM[1].xml.gz esistente.
   e. Fare clic su No.
   f. Immettere un nome univoco nel campo Nome file, quindi fare clic su Salva. Ad esempio, modificare la voce in CAELM[2].xml.gz o inserire un nome che descriva il tipo di criterio, come CAELM_EventPolicies.
   g. Fare clic su Chiudi.

      La finestra di dialogo Download completato verrà chiusa. L'elenco dei criteri resta visualizzato nel riquadro a sinistra.
4. Eseguire il backup dei criteri di scoping predefiniti come segue:
   a. Fare clic su Criteri di scoping.

      Viene visualizzata la tabella dei criteri relativa, Criteri di scoping.
   b. Fare clic sul pulsante Esporta. Potrebbe essere necessario scorrere orizzontalmente la schermata per visualizzare il pulsante nell'angolo in alto a destra.
   c. Viene visualizzata la finestra di dialogo Download file, contenente le opzioni di apertura o salvataggio.
   d. Fare clic su Salva per salvare il file.

      Viene visualizzato un messaggio che chiede se si desidera sostituire il file CAELM[1].xml.gz esistente.

e. Fare clic su No.

f. Immettere un nome univoco nel campo Nome file, quindi fare clic su Salva. Ad esempio, modificare la voce in CAELM[3].xml.gz o inserire un nome che descriva il tipo di criterio, come CAELM_CriteriScoping.

g. Fare clic su Chiudi.

La finestra di dialogo Download completato verrà chiusa. L'elenco dei criteri resta visualizzato nel riquadro a sinistra.

5. Fare clic su Chiudi.

L'elenco Criteri di accesso viene chiuso.

Esempio --CAELM[1].xml per i criteri di accesso a CALM

Di seguito viene riportata una voce per un criterio del file CAELM[1].xml.


```
  <?xml version="1.0" encoding="UTF-8" standalone="no" ?>
- <Safex>
    <Attach label="CAELM" />
    <Add />
  - <AddOrModify>
    - <Policy folder="/" name="Auditor Schedule-Annotate Rights">
        <Description>Auditors can schedule and Annotate reports</Description>
        <ResourceClassName>CALM</ResourceClassName>
        <PolicyType>policy</PolicyType>
        <Disabled>False</Disabled>
        <ExplicitDeny>False</ExplicitDeny>
        <PreDeployment>False</PreDeployment>
        <RegexCompare>False</RegexCompare>
        <Resource>Report</Resource>
        <Action>schedule</Action>
        <Action>annotate</Action>
        <Identity>ug:Auditor</Identity>
        <Attribute name="CreateTimestamp">20080926053329</Attribute>
      </Policy>
```

Ripristino dei criteri di accesso

È possibile ripristinare un criterio di accesso la cui eliminazione o modifica ha generato problemi. Se un criterio di accesso viene eliminato o danneggiato accidentalmente, gli utenti in esso indicati come Identità potrebbero non riuscire ad accedere a CA User Activity Reporting Module finché il criterio non sarà ridefinito o ripristinato.

Il ripristino dei criteri di accesso richiede l'esecuzione dell'utilità safex.

Se la propria esportazione ha creato un file di backup con estensione xml.gz oppure tar.gz, utilizzare una delle due seguenti procedure.

Per ripristinare i criteri di accesso da un backup di nome filename.xml.gz

1. Copiare i propri file di backup nella seguente directory della gestione CA User Activity Reporting Module, solitamente nel primo server installato.

   ```
   /opt/CA/LogManager/EEM
   ```

2. Eseguire il seguente comando per recuperare il file XML:

   ```
   gunzip filename.xml.gz
   ```

   Ciò creerà *filename*.xml.

3. (Facoltativo) Se si vuole ripristinare solo uno dei criteri nel gruppo sottoposto a backup, eseguire le seguenti operazioni:

   a. Aprire il file XML.

   b. Cancellare le linee XML che iniziano e finiscono con i tag seguenti per i criteri che non si desidera ripristinare:
   <Policy folder="/ name=*policyname*> e </Policy>

   c. Salvare il file.

4. Eseguire il seguente comando, in cui *eemserverhostname* si riferisce al nome di host della gestione CA User Activity Reporting Module.

   ```
   ./safex –h eemserverhostname –u EiamAdmin –p password –f filename.xml
   ```

   Se il server CA User Activity Reporting Module è in modalità FIPS, accertarsi di includere l'opzione -fips.

   Il criterio o i criteri in fase di ripristino definiti in filename.xml verranno aggiunti al tipo di criterio corretto, per poi diventare effettivi.

Per ripristinare i criteri di accesso dal backup di nome filename.tar.gz

1. Copiare i propri file di backup nella seguente directory della gestione CA User Activity Reporting Module, solitamente nel primo server installato.

   ```
   /opt/CA/LogManager/EEM
   ```

2. Eseguire il seguente comando per recuperare il file XML.

   ```
   gunzip filename.tar.gz
   ```

   Ciò creerà *filename*.tar.

3. Eseguire il comando seguente:

   ```
   tar –xvf filename.tar
   ```

   Ciò creerà *filename*.xml.

4. (Facoltativo) Se si vuole ripristinare solo uno dei criteri nel gruppo sottoposto a backup, eseguire le seguenti operazioni:

   a. Aprire il file XML.

   b. Cancellare le linee XML che iniziano e finiscono con i tag seguenti per i criteri che non si desidera ripristinare:
   <Policy folder="/ name=*policyname*> e </Policy>

   c. Salvare il file.

5. Eseguire il seguente comando, in cui *eemserverhostname* si riferisce al nome di host della gestione CA User Activity Reporting Module.

   ```
   ./safex –h eemserverhostname –u EiamAdmin –p password –f filename.xml
   ```

Per ricreare il criterio di accesso a CALM se non si dispone di alcun backup

Se non si dispone di backup, è possibile ricreare il criterio di accesso all'applicazione CALM.

1. Ricreare il criterio di accesso all'applicazione CALM. Consultare Criteri predefiniti.
2. Definire i filtri come spiegato nella seguente illustrazione. I percorsi parziali sono:
   - /CALM_Configuration/Content/Profiles
   - /CALM_Configuration/flex

Filtri

Logico	(	Tipo/valore sinistro	Operatore	Tipo/valore destro	)
NESSUNO	(	richiesta resource	STRING EQUAL ==	valore ApplicationInstance	
E		richiesta action	STRING WITHINSET {}	valore read	)
O	(	richiesta resource	STRING EQUAL ==	valore Policy	
E		richiesta action	STRING WITHINSET {}	valore read	)
O	(	richiesta resource	STRING EQUAL ==	valore User	
E		richiesta action	STRING WITHINSET {}	valore read,write	
E		attributo denominato cn	STRING EQUAL ==	richiesta identity	)
O	(	richiesta resource	STRING EQUAL ==	valore GlobalUser	
E		richiesta action	STRING WITHINSET {}	valore read	
E		attributo denominato cn	STRING EQUAL ==	richiesta identity	)
O	(	richiesta resource	STRING EQUAL ==	valore AppObject	
E		richiesta action	STRING EQUAL ==	valore read	
E		attributo denominato pozFolder	STRING CONTAINS *--*	valore /CALM_Configuration/C	)

La presenza di questo criterio consente ad ogni amministratore di accedere e di creare altri criteri.

Capitolo 4: Ruoli e criteri predefiniti

Questa sezione contiene i seguenti argomenti:

Linee guida per la creazione di criteri (a pagina 69)
Pianificazione del ruolo utente (a pagina 83)
Configurazione di ruoli utente personalizzati e criteri di accesso (a pagina 84)
Gestione di account utente e criteri di accesso (a pagina 104)
Esempio: consentire a chi non è amministratore di gestire gli archivi (a pagina 111)
Limitazione dell'accesso ai dati per un utente: scenario Win-Admin (a pagina 115)
Limitazione dell'accesso a un ruolo: scenario per analisti PCI (a pagina 129)
Criteri di esempio per le integrazioni personalizzate (a pagina 138)
Criteri di esempio per le regole di soppressione e riepilogo (a pagina 139)

Linee guida per la creazione di criteri

Tutti i criteri di accesso e di scoping di CALM definiscono le azioni consentite o negate a specifiche identità su specifiche risorse. I criteri per la classe di risorse CALM consentono o negano alle identità specificate la possibilità di eseguire azioni specifiche sulle risorse di applicazione, dette anche risorse CALM. I criteri per la risorsa AppObject di SafeObject consentono o negano alle identità specificate le operazioni di lettura e scrittura su una risorsa a livello di applicazione, come indicato nei filtri. Gli altri criteri per la classe di risorse SafeObject consentono o negano alle identità specificate le operazioni di lettura e scrittura sulle risorse globali.

Il tipo di criterio da creare dipende dalla risorsa a cui si desidera limitare l'accesso. Segue un riepilogo dei requisiti di criterio in base alla risorsa:

- Risorse che richiedono un criterio CALM e criteri di scoping per AppObject
  - Inoltro eventi
  - Raggruppamento eventi
  - Integrazione (priva di agenti)
  - Profilo
  - Rapporto

- Risorse che richiedono solo un criterio CALM
  - AgentAuthenticationKey
  - AgentConfiguration
  - Alert
  - ALL_GROUPS
  - Connettore
  - Database
  - Integrazione (relativa all'agente)
  - Tag
- Risorse che richiedono solo criteri di scoping per la risorsa globale
  - Calendar
  - Folder
  - GlobalUser
  - GlobalUserGroup
  - iPoz
  - Criterio
  - User
  - UserGroup

Le seguenti linee guida sottolineano le differenze negli approcci per la creazione di criteri, le cui differenze si basano sulle risorse che si vogliono controllare.

Per controllare l'accesso a Inoltro eventi, Raggruppamento eventi, Integrazione, Profilo e Rapporto

Il seguente approccio si applica soltanto ai criteri relativi a risorse CALM, Raggruppamento eventi, Integrazione, Profilo e Rapporto. Queste risorse applicazione richiedono un criterio CALM e due criteri di scoping.

1. Creare un criterio CALM per una o più risorse applicazione, come Rapporto o Integrazione. Indicare una o più azioni specifiche di applicazione valide per le risorse specificate come creare, pianificare o annotare. Aggiungere le identità a cui garantire o negare le azioni.
2. Creare un altro criterio di scoping sulla risorsa AppObject con entrambe le azioni di lettura e scrittura. Indicare l'azione di scrittura per consentire all'identità di modificare o eliminare la risorsa, ma non di crearla. Indicare l'azione di lettura per consentire all'identità di visualizzare o visionare la risorsa. Creare un filtro che colleghi la risorsa AppObject alla relativa risorsa applicazione. Nel filtro, specificare il percorso della cartella EEM che ospita i contenuti per la risorsa specificata, oppure che è un modulo al quale si deve accedere per ottenere la risorsa di applicazione correlata. Aggiungere a questo criterio le stesse Identità aggiunte al criterio CALM correlato.
3. Creare un secondo criterio di scoping sulla risorsa AppObject con l'azione di lettura. Indicare l'azione di lettura per consentire all'identità di visualizzare o visionare la risorsa. Creare un filtro che colleghi la risorsa AppObject alla relativa risorsa applicazione. Nel filtro, specificare il percorso della cartella EEM che ospita i contenuti per la risorsa specificata, oppure che è un modulo al quale si deve accedere per ottenere la risorsa di applicazione correlata. Aggiungere come Identità a questo criterio gli utenti o i gruppi utente con minori privilegi.

Per controllare l'accesso alle risorse Avviso, Database, Tag e relative all'agente

Il seguente approccio è valido per le risorse applicazione che richiedono solo un criterio CALM per consentire o per limitare l'accesso.

- Creare un criterio di accesso all'applicazione CALM per una risorsa come Connettore o Tag. Specificare l'azione di modifica per consentire all'identità di creare, modificare ed eliminare la risorsa, e di acquisire qualsiasi altra azione valida. Aggiungere le identità a cui assegnare o negare questa azione.

  Nota: con l'accesso alle risorse relative all'agente vengono abilitati i pulsanti della cartella Explorer agente o della sottoscheda Raccolta registri della scheda Amministrazione. L'accesso alla risorsa Avviso consente all'Identità di accedere alla scheda Avvisi. L'accesso alla risorsa Tag consente all'Identità di creare un tag per una query o per un rapporto personalizzati. L'accesso a Database consente all'Identità di eseguire una query di archiviazione.

Per controllare l'accesso alle risorse globali utilizzate nell'applicazione CAELM

Il seguente approccio vale per le risorse globali, che richiedono solo un criterio di scoping per limitare l'accesso.

1. Creare un criterio di scoping per una o più risorse globali come Utente o Criterio. Indicare l'azione di scrittura per consentire all'Identità di creare, modificare o eliminare la risorsa. Aggiungere le identità a cui assegnare o negare questa azione.
2. Creare un criterio di scoping per una o più risorse globali come Utente o Criterio. Indicare l'azione di lettura per consentire all'Identità di visualizzare la risorsa globale. Aggiungere le identità a cui assegnare o negare questa azione.

   Nota: sono disponibili risorse globali dotate di pulsanti nella sottoscheda Gestione utenti e accessi della scheda Amministrazione.

Ulteriori informazioni:

Tipi di criteri di accesso di CALM (a pagina 73)
Risorse ed azioni (a pagina 76)
Risorse CALM e cartelle EEM (a pagina 79)
Risorse globali e Funzionalità CA EEM (a pagina 82)
Creazione di un criterio di accesso a CALM (a pagina 91)

Tipi di criteri di accesso di CALM

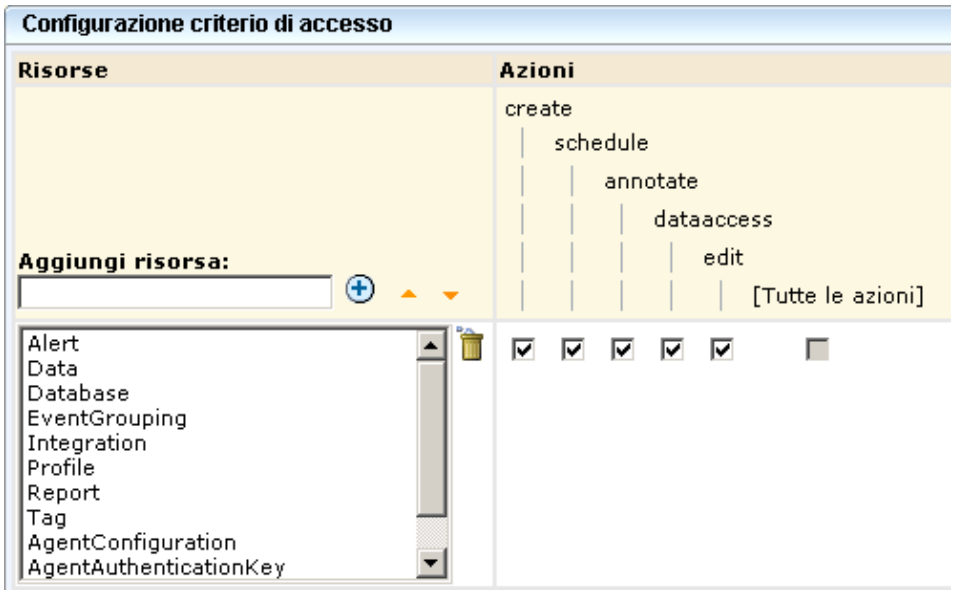
Quando si crea un criterio di accesso a CALM o un criterio di scoping, è possibile selezionare uno dei seguenti tre tipi:

- Criterio di accesso
- Elenco di controllo di accesso
- Elenco di controllo di accesso identità

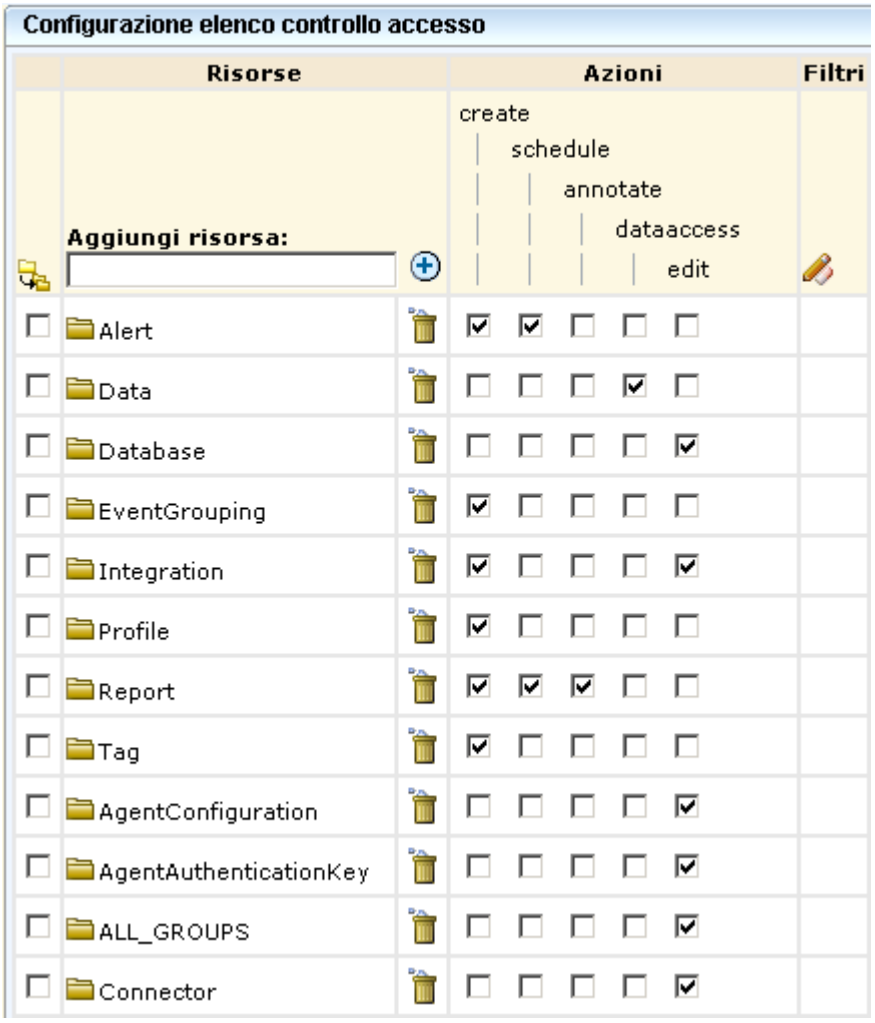
Tale scelta influisce sul livello di dettaglio della configurazione dei criteri di accesso, in cui il più ampio è il criterio di accesso.

Nota: gli esempi mostrati sono criteri di accesso per la classe di risorsa CALM, e pertanto comprendono azioni e risorse specifiche di CA User Activity Reporting Module.

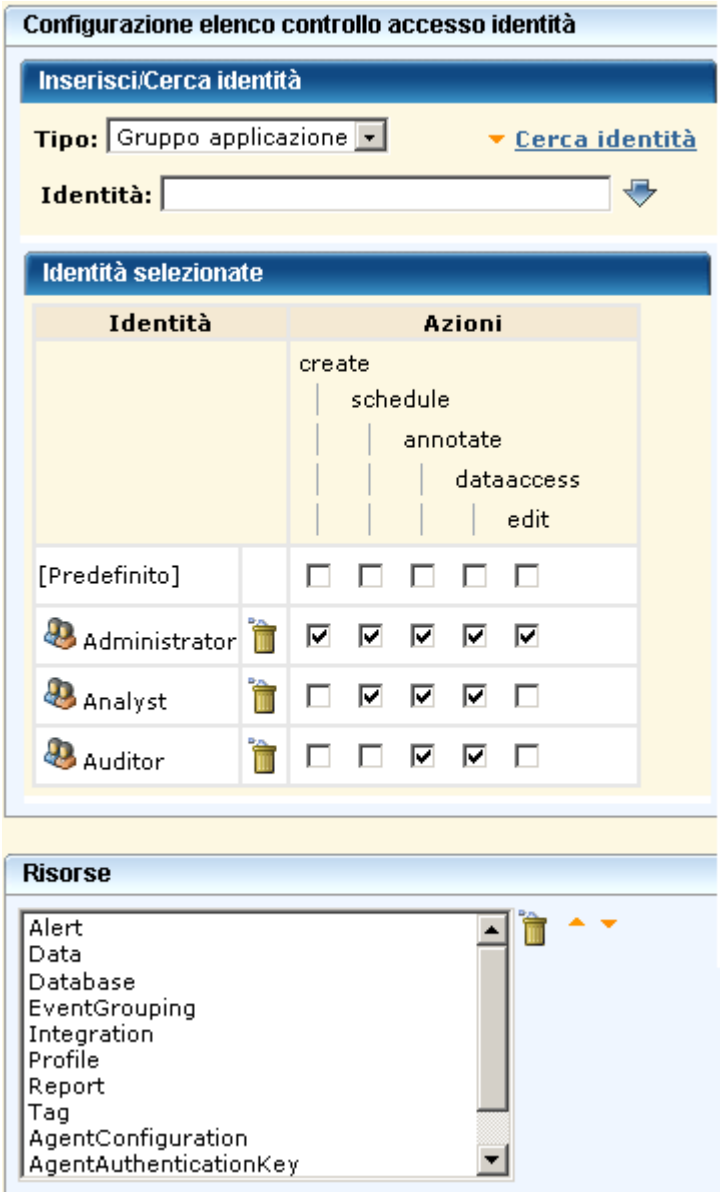
Un criterio di accesso specifica le azioni che è possibile eseguire per ogni risorsa selezionata conferita a tutte le identità selezionate. Quando si crea un criterio generico per CA User Activity Reporting Module, si aggiungono risorse appartenenti alla classe di risorsa CALM, e si possono quindi selezionare azioni dall'elenco visualizzato. Le azioni selezionate si applicano alle risorse selezionate per cui esse sono valide. In questo esempio, il criterio consente di eseguire ogni azione selezionata su tutte le risorse selezionate per cui Crea è valido.



Un elenco di controllo accesso specifica le azioni valide per ogni risorsa per le singole identità selezionate. Creando un criterio incentrato sulla risorsa, è possibile specificare quali azioni consentire su ogni risorsa. Non occorre selezionare le azioni per una data risorsa solo perchè esse sono valide. Per esempio, è possibile consentire Crea per i rapporti ma non per gli avvisi, anche se Crea è un'azione valida per gli avvisi. L'elenco di controllo di accesso è il criterio più raffinato, a patto di implementarlo su di un'identità alla volta.



Un elenco di controllo accessi identità consente di specificare le azioni consentite alle identità selezionate per tutte le risorse selezionate applicabili. Quando si crea un criterio incentrato sull'identità, indicare quali identità possano eseguire determinate azioni (creare, pianificare, annotare e modificare) su tutte le risorse elencate cui è possibile applicare ogni azione. Se si desidera impedire al revisore di pianificare gli avvisi, si deve lasciare vuota la pianificazione. Tuttavia, lasciando vuota la pianificazione si impedirebbe al revisore anche di pianificare i rapporti.



Risorse ed azioni

Quando si creano criteri, configurare un criterio di accesso per cui è necessario un filtro di accesso. Un filtro di accesso è un filtro che l'amministratore può impostare per controllare quali dati evento possano essere visualizzati dagli utenti e dai gruppi non amministrativi. Ad esempio, un filtro di accesso può limitare i dati presenti sui rapporti visualizzati da determinati utenti o gruppi. I filtri di accesso saranno convertiti automaticamente in Criteri di obbligo EEM. Spesso i filtri di accesso sono espressi nei termini dei percorsi relativi agli oggetti con accesso limitato da parte dell'utente. È possibile visualizzare questi percorsi relativi nell'area Cartelle EEM dell'interfaccia.

Di solito, i criteri che autorizzano azioni come la creazione e la pianificazione vengono definiti con la classe di risorsa CALM e risorse CALM quali rapporti, tag, file DM ed MP, regole di soppressione e riepilogo. I criteri che autorizzano le azioni di lettura e scrittura si definiscono con la classe di risorsa SafeObject e con la risorsa AppObject. L'azione Modifica è l'unica valida per le risorse relative all'agente nella classe di risorsa CALM.

Più in dettaglio, le azioni che è possibile autorizzare per gli oggetti appartenenti alla risorsa CALM sono le seguenti:

Azione	Resource	Descrizione
Annotazione	Rapporto	Registrare i commenti sui rapporti.
Creazione	Inoltro eventi	Creare regole per inoltrare eventi specifici a specifiche applicazioni di terze parti.
Creazione	EventGrouping	Creare regole di soppressione e di riepilogo utilizzando la Grammatica evento comune.
Creazione	Integrazione	Creare file di mapping dei dati e di analisi del messaggio utilizzando la Grammatica evento comune.
Creazione	Profilo	Creare profili
Creazione	Rapporto	Creare rapporti e query.
Creazione	Tag	Creare tag per rapporti e query.
Dataaccess	Dati	Accedere ai dati d'evento CALM, che si possono limitare con dei filtri d'accesso dei dati.
Modifica	AgentConfiguration	Creare gruppi di agenti. Configurare gli agenti installati con origini per la raccolta e destinazione per l'elaborazione.

Azione	Resource	Descrizione
Modifica	AgentAuthenticationKey	Creare e modificare la chiave di autenticazione agente specificata durante l'installazione dell'agente.
Modifica	ALL_GROUPS	Modificare tutti i gruppi di agenti disponibili. **Nota:** è possibile limitare l'accesso ad un particolare gruppo di agenti indicando il nome del Gruppo di agenti come risorsa.
Modifica	Connettore	Configurare i connettori.
Modifica	Database	Definire i registri esistenti che corrispondono ai criteri Query di catalogo archiviazioni e ricatalogare il database.
Modifica	Integrazione	Modificare i dettagli di integrazione.
Pianificazione	Alert	Pianificare gli avvisi.
Pianificazione	Rapporto	Pianificare i rapporti e le query.

Le seguenti azioni consentono agli utenti di visualizzare o di modificare un oggetto appartenente alla risorsa SafeObject:

Azione	Resource	Descrizione
Lettura	AppObject	Visualizzare modelli di rapporto e di query, tag, processi di rapporto pianificati, processi di avviso, configurazioni di servizio, file di mapping dei dati (DM), file di analisi dei messaggi (XMP) e regole di inoltro degli eventi.
Lettura	Calendar	Visualizzare i calendari elencati sotto Amministrazione, Gestione utenti e accessi, Calendari.
Lettura	Folder	Visualizzare le cartelle elencate sotto Amministrazione, Gestione utenti e accessi, Cartelle EEM.
Lettura	GlobalUser	Visualizzare le informazioni sugli utenti elencati al momento di eseguire una query per Utenti globali sotto Amministrazione, Gestione utenti e accessi, Utenti.
Lettura	iPoz	Visualizzare le impostazioni dell'archivio utente sotto Amministrazione, Gestione utenti e accessi, Archivio utente. Visualizzare le impostazioni del criterio di password sotto Amministrazione, Gestione utenti e accessi, Criteri di password.

Azione	Resource	Descrizione
Lettura	Criterio	Visualizzare i criteri elencati sotto Amministrazione, Gestione utenti e accessi, Criteri di accesso.
Lettura	User	Visualizzare Dettagli utente quando si ricerca Dettagli utente applicazione sotto Amministrazione, Gestione utenti e accessi, Utenti.
Lettura	UserGroup	Visualizzare l'appartenenza al gruppo applicazione per gli utenti elencati quando si ricerca Dettagli utente applicazione sotto Amministrazione, Gestione utenti e accessi, Utenti.
Scrittura	AppObject	Visualizzare modelli di rapporto e di query, tag, processi di rapporto pianificati, processi di avviso, configurazioni di servizio, file di mapping dei dati (DM), file di analisi dei messaggi (XMP) e regole di inoltro degli eventi.
Scrittura	Calendar	Modificare i calendari definiti dall'utente.
Scrittura	Folder	Modificare i dati definiti dall'utente aggiunti alla struttura di cartelle EEM.
Scrittura	GlobalUser	Modificare i dettagli utente globali.
Scrittura	iPoz	Configurare l'archivio utente e i criteri di password.
Scrittura	Criterio	Modificare i criteri predefiniti e definiti dall'utente.
Scrittura	User	Modificare i dettagli utente applicazione.
Scrittura	UserGroup	Creare, modificare ed eliminare un gruppo utente dell'applicazione.

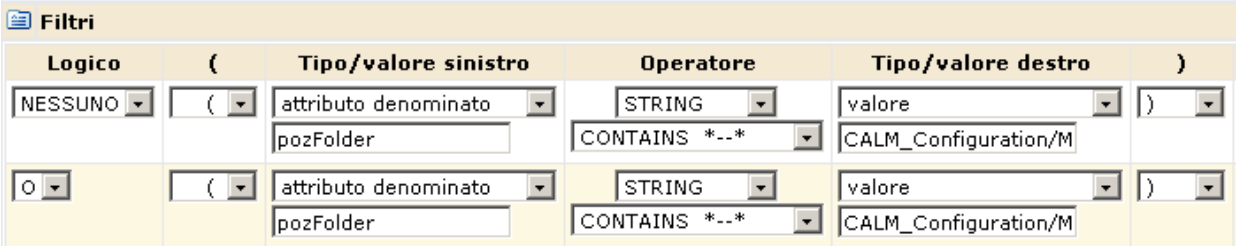
Risorse CALM e cartelle EEM

Per ogni criterio personalizzato di CALM creato da zero che comprenda InoltroEventi, RaggruppamentoEventi, Integrazione, Profilo o Rapporto, è possibile creare un criterio di scoping su AppObject. Il criterio di scoping dispone di un accesso in lettura e in scrittura che consente di filtrare i percorsi EEM di ogni risorsa CALM elencata nel criterio corrispondente. A questo criterio si assegneranno come Identità gli stessi gruppi utente che sono Identità per il criterio CALM. Per completare il gruppo di criteri, creare un criterio aggiuntivo di scoping di sola lettura, assegnare un'identità in grado di visualizzare soltanto la risorsa, ed inserire un filtro con un percorso di cartella EEM.

Nota: se un criterio CALM richiede il supporto di un criterio di scoping, ciò dipende dalla risorsa utilizzata dal criterio CALM. Ad esempio, Database, Tag ed Avviso sono risorse CALM che non richiedono alcun criterio di scoping. I criteri di scoping non sono necessari neppure per le risorse relative agli agenti.

È possibile visualizzare le cartelle EEM dalla scheda Amministrazione e dalla sottoscheda Gestione Gestione utenti e accessi. Selezionando una cartella come Soppressione, verrà visualizzato tale percorso. Consultare l'esempio seguente:

Si specifica il percorso della cartella EEM come valore in un'espressione che inizia con pozFolder CONTAINS, come mostrato nella sezione Filtri di una definizione di criterio. Segue un esempio:



Le seguenti tabelle forniscono delle linee guida per i valori specificati nel filtro di un criterio di scoping correlato ad uno di CALM che consenta o neghi l'accesso a specifiche risorse CALM.

Nota: non esiste una corrispondenza diretta fra risorse e cartelle CALM.

Quando si crea un criterio di scoping che consenta l'accesso al contenuto di questa risorsa CALM	Aggiungere un filtro che indichi questo percorso di cartella EEM
Inoltro eventi	pozFolder CONTAINS /CALM_Configuration/Content/Rules/Forwarding
EventGrouping	pozFolder CONTAINS /CALM_Configuration/Content/Rules/Summarization pozFolder CONTAINS /CALM_Configuration/Content/Rules/Suppression
Integrazione (Server)	pozFolder CONTAINS /CALM_Configuration/Content/Mapping pozFolder CONTAINS /CALM_Configuration/Content/Parsing
Profilo	pozFolder CONTAINS /CALM_Configuration/Content/Profiles
Rapporto	pozFolder CONTAINS /CALM_Configuration/Content/CEG pozFolder CONTAINS /CALM_Configuration/Content/Reports

Quando si crea un criterio di scoping che richieda l'accesso a questo modulo CALM	Aggiungere un filtro che indichi questo percorso di cartella EEM
Gestione agente	pozFolder CONTAINS /CALM_Configuration/Modules/AgentManager
Archivio registro eventi	pozFolder CONTAINS /CALM_Configuration/Modules/logDepot

Quando si crea un criterio di scoping che richieda l'accesso a questo modulo CALM	Aggiungere un filtro che indichi questo percorso di cartella EEM
Server di rapporto	pozFolder CONTAINS /CALM_Configuration/Modules/calmReporter
Modulo di sottoscrizione	pozFolder CONTAINS /CALM_Configuration/Modules/Subscription

Risorse globali e Funzionalità CA EEM

È possibile creare un criterio di scoping simile negli obiettivi ad un criterio CALM, ad eccezione del fatto che le risorse sono globali e non specifiche di prodotto. Le risorse globali sono quelle utilizzate in più prodotti CA. È possibile creare criteri per consentire o negare l'accesso a risorse globali specifiche, accessibili tramite i pulsanti disponibili nella sottoscheda Gestione utenti e accessi della scheda Amministrazione.

Utilizzare la seguente tabella come guida per la creazione di un criterio di scoping per concedere o negare a specifiche identità la capacità di lettura e scrittura se la risorsa specificata è una risorsa globale.

Attività	Azione	Risorsa globale
Mostrare, creare, modificare o eliminare un utente globale, un gruppo utente globale e un gruppo utente dell'applicazione (ruolo). Aggiungere un gruppo applicazione (ruolo) ad un utente globale oppure creare un utente globale con un ruolo.	read, write	User UserGroup GlobalUser GlobalUserGroup
Creare, modificare, copiare, esportare, disattivare, verificare, visualizzare o eliminare un criterio. Aggiungere un calendario ad un criterio.	read, write	Criterio Calendar
Creare, modificare, copiare, visualizzare o eliminare un filtro di accesso. Visualizzare le cartelle EEM.	read, write	Criterio
Creare un calendario.	read, write	Calendar
Configurare l'archivio utente. Creare, modificare o visualizzare i criteri di password.	read, write	iPoz

Nel creare un filtro per una risorse globale, fare riferimento come esempio al filtro per il criterio di Accesso all'applicazione CALM. Una delle azioni eseguite dal filtro è specificare l'associazione fra azioni e risorse. Facendo clic su Modifica su un criterio predefinito, sarà possibile esaminare l'origine di un esempio sull'inserimento della logica.

Pianificazione del ruolo utente

Se i gruppi utente dell'applicazione predefiniti, ovvero amministratore, analista e revisore, non sono sufficienti per la proprie esigenze, è possibile creare ruoli personalizzati con nuovi gruppi utente dell'applicazione. Ad esempio, per assegnare un piccolo gruppo di individui alla gestione degli account utente, premesso che questi individui non hanno accesso alla funzionalità non correlata di CA User Activity Reporting Module, è possibile definire un ruolo UserAccountAdministrator, creare un criterio di scoping per quel ruolo, aggiungerlo al criterio di accesso per l'applicazione CALM e assegnarlo agli utenti incaricati di gestire gli account utente.

La pianificazione degli utenti CALM prevede i passaggi seguenti:

- Determinazione del numero di utenti necessari per amministrare, analizzare e controllare CA User Activity Reporting Module.
- Identificazione degli utenti cui garantire l'accesso a CA User Activity Reporting Module.

Se si ha intenzione di creare ruoli personalizzati con criteri di accesso associati, considerare l'approccio seguente:

- Identificare il ruolo a cui assegnare ogni utente CA User Activity Reporting Module.
- Identificare il tipo di accesso alle risorse CA User Activity Reporting Module richiesto per ogni ruolo.

È anche possibile considerare le alternative seguenti ai ruoli definiti dall'utente (gruppi delle applicazioni):

- Configurazione di criteri gruppo utente dinamici che creino gruppi utente dinamici.
- Creazione di gruppi globali da considerarsi come gruppi dell'applicazione. Questo significa assegnarli agli utenti e successivamente ai criteri come identità.

  Questo approccio può essere utile se i criteri vengono creati allo scopo di limitare l'accesso per posizione geografica e se si vuole che gli stessi utenti abbiano lo stesso livello di diritti su più prodotti CA. Ad esempio, un criterio di gruppo per Location-A_Admin avrebbe potuto essere assegnato agli utenti che dovevano amministrare diversi prodotti CA nella Location-A. È possibile creare per ogni prodotto CA criteri che garantiscano diritti da amministratore per i server su cui tale prodotto è stato installato nella Location-A.

Ulteriori informazioni:

Creazione di un gruppo globale (a pagina 38)

Configurazione di ruoli utente personalizzati e criteri di accesso

Un *ruolo utente* può essere un gruppo applicazione predefinito o un gruppo applicazione definito dall'utente. Sono necessari ruoli utente personalizzati quando i gruppi applicazione predefiniti (amministratore, analista e revisore) non sono sufficientemente dettagliati per riflettere le assegnazioni del lavoro. I ruoli utente personalizzati richiedono criteri di accesso personalizzati e la modifica dei criteri predefiniti per includere il nuovo ruolo.

Gli amministratori possono creare ruoli utente e i criteri corrispondenti con la modalità seguente:

1. Per ogni ruolo assunto dagli utenti di CA User Activity Reporting Module:
   - Identificare le risorse cui garantire l'accesso.
   - Identificare le azioni da consentire per ogni risorsa.
   - Identificare le identità o gli individui a cui applicare questo ruolo.

     Nota: le identità possono essere altri gruppi applicazione concepiti per costituire un supergruppo.

2. Se un gruppo applicazione predefinito è troppo esteso per le necessità dell'utente, creare un nuovo gruppo e assegnarlo agli individui identificati. È consigliabile denominare un gruppo applicazione definito dall'utente con un termine che descriva il ruolo che gli utenti assegnati devono avere.
3. Aggiungere il nuovo gruppo applicazione al criterio di accesso per l'applicazione CALM, un tipo di elenco Access Control.
4. Se il nuovo ruolo deve poter eseguire azioni su una o più risorse, come la creazione, seguire questa procedura:
   a. Configurare un criterio CALM che consenta al nuovo gruppo applicazione di creare o realizzare altre azioni valide relative alle risorse CA User Activity Reporting Module identificate.
   b. Configurare un criterio di scoping che garantisca al nuovo gruppo applicazione accesso di lettura e scrittura alla risorsa AppObject e specificare un filtro che preveda la posizione in cui la risorsa identificata verrà memorizzata nelle cartelle EEM. Per ogni filtro, inserire l'attributo denominato, pozFolder, CONTAINS e un valore, dove tale valore è il percorso della cartella EEM che inizia con /CALM_Configuration.
5. Se il nuovo ruolo necessita soltanto di visualizzare una risorsa CA User Activity Reporting Module specifica, configurare un criterio di scoping che consenta l'accesso di lettura ad AppObject e specificare un filtro in cui l'attributo denominato, pozFolder, contenga (CONTAINS) un valore, ovvero il percorso della cartella EEM che inizia con /CALM_Configuration in cui è archiviata la risorsa.
6. Testare i criteri.
7. Assegnare il nuovo ruolo agli account utente.

Gli amministratori possono anche creare accessi utente limitati con filtri di accesso. Se un tipo specifico di accesso limitato si applica soltanto a una persona, si può evitare di assegnarla a un gruppo applicazione o a un ruolo. Per limitare l'accesso di un utente:

1. Creare un utente senza assegnare a esso alcun ruolo.
2. Consentire all'utente l'accesso all'applicazione CA User Activity Reporting Module aggiungendolo al criterio di accesso CALM.
3. Creare un criterio di scoping che garantisca l'accesso di lettura o scrittura a SafeObject e AppObject e specificare un filtro in cui l'attributo denominato pozFolder corrisponda al valore della cartella EEM per la risorsa. Ad esempio, se la risorsa sono i rapporti, impostare l'attributo denominato calmTag in modo che sia uguale al valore di un tag di rapporto.
4. Creazione di un filtro di accesso personalizzato

Gli amministratori possono personalizzare l'accesso utente alle risorse CA User Activity Reporting Module. Considerare gli esempi riportati di seguito:

- Creazione di ruoli per assegnare responsabilità di amministrazione specifiche a gruppi diversi di amministratori. Ad esempio, creare un ruolo come UserAccountAdministrator. Creare un criterio che garantisca agli utenti con questo ruolo l'accesso alla sola funzionalità necessaria per gestire utenti e gruppi. Questo criterio deve definire l'accesso di lettura e scrittura alla risorsa GlobalUser e alle risorse User e UserGroup.
- Creazione di ruoli per distribuire le responsabilità degli analisti ai vari tipi di report e query basati sui tag. Ad esempio, creare ruoli come SystemAccessAnalyst e PCIAnalyst e assegnare gli analisti a uno solo dei ruoli analista limitati. Quindi, creare criteri che garantiscano l'accesso a un sottoinsieme di queste risorse basato sui tag. Ad esempio, creare un criterio che garantisca al ruolo SystemAccessAnalyst accesso ai rapporti e alle query con il tag Accesso al sistema e un altro che garantisca al ruolo PCIAnalyst di accedere ai rapporti e alle query con il tag PCI. Creare altri ruoli e criteri basati su altri tag. Per limitare l'accesso in questo modo, i criteri utilizzano filtri di accesso.

Gli amministratori possono creare criteri basati sul server nei modi seguenti:

- Limitazione dei dati

  È possibile restringere l'accesso a registri specifici creando un filtro di accesso ai dati, impostando il filtro per il campo receiver_name e specificando un valore come systemstatus o syslog.

- Limitazione della configurazione

  È possibile limitare l'accesso a un particolare server CA User Activity Reporting Module tramite la creazione di un criterio sulla classe di risorse SafeObject con AppObject come risorsa selezionata. Questo significa che, per limitare l'accesso solo alla configurazione del server di rapporto su un host specifico, è necessario definire un filtro come segue:

  ```
  pozFolder contains /CALM_Configuration/Modules/calmReporter/LogServer01
  ```

Ulteriori informazioni:

Criteri di esempio per le integrazioni personalizzate (a pagina 138)
Criteri di esempio per le regole di soppressione e riepilogo (a pagina 139)
Creazione di un filtro di accesso (a pagina 103)
Limitazione dell'accesso ai dati per un utente: scenario Win-Admin (a pagina 115)
Limitazione dell'accesso a un ruolo: scenario per analisti PCI (a pagina 129)

Creazione di un gruppo utente delle applicazioni (ruolo)

È possibile creare un nuovo gruppo utente dell'applicazione per supportare i ruoli necessari. Una volta creato un nuovo gruppo utente dell'applicazione, è necessario creare criteri di accesso per tale gruppo.

Un caso in cui i nuovi criteri di accesso non sono richiesti per un nuovo gruppo è quando a quel gruppo viene data l'appartenenza a gruppi esistenti. Prendere in considerazione la situazione in cui è necessario un ruolo per gli utenti che si dedicano alla creazione di file di mapping di dati e analisi di messaggi, un altro ruolo per chi si occupa delle regole di soppressione e di eliminazione e un terzo per chi può eseguire entrambe queste attività. Si potrebbe definire un solo gruppo utente dell'applicazione chiamato AdminDMMP con un criterio che garantisca l'accesso di creazione alla risorsa Integration e un altro gruppo chiamato AdminSS con un criterio che garantisca l'accesso di creazione alla risorsa EventGrouping. Successivamente, si potrebbe creare un terzo gruppo chiamato AdminDMMPSS con appartenenza ai gruppi AdminDMMP e AdminSS. Questo terzo gruppo erediterebbe automaticamente i criteri dai due gruppi di appartenenza.

Anziché creare nuovi gruppi o ruoli dell'applicazione, è possibile espandere i ruoli predefiniti di analista e revisore. Ad esempio, se si vuole che gli analisti siano in grado di creare regole di soppressione e riepilogo e che i revisori possano visualizzare tali regole, è possibile creare un criterio CALM che garantisca la capacità di creare regole di soppressione e riepilogo e un criterio di scoping che conceda la capacità di visualizzare o modificare regole personalizzate e poi assegnare il ruolo di analista a tali criteri. A questo punto, è possibile creare un criterio di scoping che garantisca agli utenti la capacità di visualizzare regole di soppressione e riepilogo e poi assegnare il gruppo revisore a tale criterio.

Soltanto gli amministratori possono creare nuovi ruoli.

Per creare un nuovo gruppo utenti dell'applicazione (ruolo)

1. Fare clic sulla scheda Amministrazione e sulla sottoscheda Gestione utenti e accessi.
2. Fare clic su Gruppi.
3. Fare clic sul pulsante Nuovo gruppo dell'applicazione posto a sinistra della cartella Gruppi applicazione dell'elenco Gruppi utente.
4. Fornire il nome e la descrizione del gruppo.

5. Se questo nuovo gruppo utente deve avere accesso già definito a due o più gruppi dell'applicazione definiti dall'utente, selezionare tali gruppi. Altrimenti, non apportare alcuna selezione.

   Nota: se questo nuovo gruppo è composto di gruppi esistenti, i criteri esistenti per ognuno dei gruppi componenti varranno anche per tale gruppo. Non è richiesto alcun criterio aggiuntivo.

6. Fare clic su Salva.
7. Fare clic su Chiudi.

Ulteriori informazioni:

Passaggio 2: creazione del ruolo Analista PCI (a pagina 132)
Criteri di esempio per le regole di soppressione e riepilogo (a pagina 139)

Come garantire l'accesso ruolo personalizzato a CA User Activity Reporting Module

Quando si crea un gruppo utente dell'applicazione, o ruolo, assicurarsi di aggiungerlo al criterio di accesso all'applicazione CALM predefinito. Soltanto le identità aggiunte esplicitamente a questo criterio possono accedere a CA User Activity Reporting Module. Può trattarsi di utenti individuali o membri di un gruppo utente.

Se si verifica una situazione in cui gli utenti assegnati a un nuovo gruppo utente non riescono ad accedere a CA User Activity Reporting Module, verificare che le identità del criterio di accesso all'applicazione CALM includano tale gruppo.

Per garantire l'accesso a CA User Activity Reporting Module ai gruppi utente dell'applicazione definiti dall'utente

1. Selezionare la scheda Amministrazione, fare clic su Gestione utenti e accessi, quindi su Criteri di accesso nel riquadro sinistro.
2. Fare clic su Criteri di scoping e selezionare Accesso all'applicazione CALM.

3. In Identità, cercare il nuovo gruppo applicazione come segue:
   a. Per tipo, selezionare Gruppo applicazione.
   b. Fare clic su Cerca identità.
   c. Lasciare Nome come attributo e LIKE come operatore. Fare clic su Cerca.

      Il nome del nuovo gruppo applicazione compare nell'elenco di identità visualizzato.
   d. Selezionare il nome del nuovo gruppo applicazione e fare clic sul pulsante Sposta per spostare il nome del gruppo nella casella Identità selezionate.
4. Fare clic su Salva.

Aggiunta di un'identità a un criterio esistente

Quando si crea un nuovo gruppo utente dell'applicazione, è possibile aggiungerlo ai criteri esistenti, se applicabili. Quando si crea un utente privo di ruolo ma con accesso limitato da un filtro di accesso, è possibile aggiungerlo ai criteri esistenti.

Importante: Quando si lavora con i criteri di accesso installati, prestare attenzione a non cancellarli nel caso in cui non siano bloccati o protetti.

Se un criterio di accesso predefinito viene eliminato inavvertitamente, gli utenti non saranno in grado di accedere al server CA User Activity Reporting Module finché non verrà ripristinato. È possibile ripristinare i criteri che utilizzano l'utilità safex.

Per aggiungere un'identità a un criterio esistente

1. Selezionare la scheda Amministrazione, fare clic su Gestione utenti e accessi, e quindi fare clic su Criteri di accesso nel riquadro di sinistra.
2. Fare clic sul tipo di criterio e selezionare il criterio adeguato per il nuovo gruppo utenti dell'applicazione. Visualizzare il riquadro Identità.
3. Per Tipo, selezionare Gruppo applicazione.
4. Fare clic su Cerca identità.
5. Lasciare Nome come attributo e LIKE come operatore. Fare clic su Cerca.

   Il nome del nuovo gruppo applicazione compare nell'elenco di identità visualizzato.
6. Selezionare il nome del nuovo gruppo applicazione e fare clic sul pulsante Sposta per spostare il nome del gruppo nella casella Identità selezionate.
7. Fare clic su Salva.

Ulteriori informazioni:

Passaggio 4: aggiunta dell'analista PCI ai criteri esistenti (a pagina 133)

Creazione di un criterio di accesso a CALM

È possibile creare un criterio di accesso CALM per garantire (o negare) una o più azioni valide su una o più risorse CALM.

Le seguenti risorse CALM sono specifiche dell'applicazione, ovvero vengono usate soltanto dal prodotto CA User Activity Reporting Module:

- Alert
- AgentConfiguration
- AgentAuthenticationKey
- ALL_GROUPS
- Connettore
- Dati
- Database
- EventGrouping
- Integrazione
- Profilo
- Rapporto
- Tag

Per creare da zero un nuovo criterio CALM

1. Fare clic sulla scheda Amministrazione e sulla sottoscheda Gestione utenti e accessi.
2. Fare clic su Criteri di accesso.
3. Fare clic sul pulsante Nuovo criterio di accesso, a sinistra della cartella di CALM.
4. Inserire un nome significativo per il criterio e, facoltativamente, una breve descrizione.
5. Se il criterio è temporaneo, selezionare il calendario con l'intervallo di date cui si applicherà tale criterio.
6. Accettare CALM come nome di classe risorsa.

7. Selezionare Tipo nel pannello Generale, in base ai seguenti criteri:
   - Selezionare il criterio di accesso per garantire o negare a tutte le identità selezionate la possibilità di eseguire tutte le azioni selezionate su tutte le risorse selezionate a cui esse sono applicabili.
   - Selezionare l'elenco controllo di accesso per garantire o negare a tutte le identità selezionate la possibilità di eseguire solo le azioni selezionate su una risorsa selezionata.

     Nota: è impossibile salvare i filtri per più risorse. Per aggirare il problema è possibile creare criteri separati, uno per ogni combinazione di risorsa e filtri.
   - Selezionare l'elenco controllo di accesso dell'identità per garantire o negare ad ogni identità selezionata la possibilità di eseguire le azioni selezionate su tutte le risorse selezionate a cui esse si possono applicare.
8. Utilizzare l'area Identità per selezionare gli utenti o i gruppi a cui applicare questo criterio, e precisamente:
   a. Selezionare Gruppo applicazione per Tipo o una delle altre opzioni, fare clic su Cerca identità e quindi su Cerca.
   b. Selezionare le identità fra quelle disponibili, e fare clic sul pulsante Sposta per ricollocarle nella casella Identità selezionate.
9. Se il tipo di criterio è di accesso, completarne la configurazione come segue:
   a. Inserire una risorsa CALM nel campo Aggiungi risorsa, e fare clic su Aggiungi.
   b. Selezionare ogni azione che le identità selezionate potranno eseguire su ogni risorsa selezionata. Le azioni valide comprendono le seguenti: annotare, creare, dataaccess, modificare e pianificare. Non è possibile garantire l'esecuzione di una data azione su una risorsa e non su un'altra su cui essa è valida.

10. Se il tipo di criterio è elenco controllo di accesso, completare la relativa configurazione come segue:
    a. Inserire una risorsa CALM nel campo Aggiungi risorsa, e fare clic su Aggiungi.
    b. Selezionare ogni azione che le identità selezionate potranno eseguire su questa risorsa. Saranno valide una o più azioni fra le seguenti: annotare, creare, dataaccess, modificare e pianificare.
    c. Ripetere gli ultimi due passaggi per ogni risorsa da indirizzare con questo criterio.

       Con questo tipo, è possibile garantire l'esecuzione di un'azione, come ad esempio Crea, su una risorsa ma non su un'altra.
11. Se il tipo di criterio è elenco controllo di accesso identità, completare la configurazione relativa come segue:
    a. Per ogni identità selezionata, scegliere le azioni da garantire o da negare su tutte le risorse per cui esse sono valide.
    b. Per ogni risorsa da aggiungere, inserire un nome risorsa CALM nel campo Aggiungi risorsa, e fare clic su Aggiungi:
12. Controllare le caselle di controllo nella parte superiore della pagina e selezionare quelle adatte:
    - Selezionare Negazione esplicita per modificare un criterio che consenta l'accesso in uno che lo neghi.
    - Selezionare Inattivo per disattivare temporaneamente questo criterio, a patto che esso sia nuovo.
    - Selezionare Distribuzione preliminare e quindi Assegna etichette per aggiungere delle etichette, a patto che si utilizzi questo criterio per motivi di verifica, e che si desideri ripartire i criteri in categorie usando etichette personalizzate.
13. Nel riquadro di sinistra, fare clic su Salva e quindi su Chiudi.

Creazione di un criterio di scoping

È possibile creare un criterio di scoping su qualsiasi risorsa globale. Le azioni sui criteri di scoping sono limitate alla lettura e alla scrittura.

- Molti prodotti CA (applicazioni) utilizzano le seguenti risorse globali:
  - Calendar
  - GlobalUser
  - GlobalUserGroup
  - iPoz
  - Criterio
  - User
  - UserGroup
  - AppObject
- La risorsa globale AppObject consente di creare criteri di scoping su risorse e moduli specifici di applicazione. Per fare ciò occorre aggiungere un filtro che determini la cartella EEM appropriata in cui saranno memorizzati i contenuti o i moduli specifici di applicazione.
  - Nei filtri con la risorsa AppObject è possibile utilizzare le seguenti cartelle di contenuto EEM:
    - EventGrouping
    - Integrazione (Server)
    - Profilo
    - Rapporto
  - Nei filtri con la risorsa AppObject è possibile utilizzare le seguenti cartelle di modulo CA User Activity Reporting Module:
    - Archivio registro eventi
    - Server di rapporto
    - Sottoscrizione

È possibile creare un criterio da zero se non ne esiste nessuno da cui acquisire le impostazioni. Se si sta creando un criterio di scoping associato ad un criterio CALM già creato, specificare le stesse identità del criterio CALM correlato.

Soltanto gli amministratori possono creare, modificare, eliminare e visualizzare i criteri di accesso.

Per creare un nuovo criterio di scoping di assegnazione esplicita

1. Fare clic sulla scheda Amministrazione e sulla sottoscheda Gestione utenti e accessi.
2. Fare clic su Criteri di accesso.
3. Fare clic sul pulsante Nuovo criterio di scoping, a sinistra della cartella Criteri di scoping.
4. Creare un nome significativo per il criterio. Ad esempio, inserire il ruolo o i ruoli a cui esso si può applicare e le attività soggette a scoping. Visualizzare i nomi dei criteri predefiniti per ottenere degli esempi su come utilizzare questo standard.
5. Inserire una breve descrizione che illustri in maniera completa il significato di un nome poco chiaro.
6. Di solito, come nome di classe di risorsa verrà accettato SafeObject.
7. Selezionare Tipo nel pannello Generale, in base ai seguenti criteri:
   - Selezionare il criterio di accesso per garantire o negare a tutte le identità selezionate la possibilità di eseguire tutte le azioni selezionate su tutte le risorse selezionate a cui esse sono applicabili.
   - Selezionare l'elenco controllo di accesso per garantire o negare a tutte le identità selezionate la possibilità di eseguire solo le azioni selezionate su una risorsa selezionata.

     Nota: è impossibile salvare i filtri per più risorse. Per aggirare il problema è possibile creare criteri separati, uno per ogni combinazione di risorsa e filtri.
   - Selezionare l'elenco controllo di accesso dell'identità per garantire o negare ad ogni identità selezionata la possibilità di eseguire le azioni selezionate su tutte le risorse selezionate a cui esse si possono applicare.
8. Se il tipo di criterio è accesso oppure elenco di controllo di accesso, utilizzare l'area Identità per selezionare gli utenti o i gruppi a cui esso si applica.
   a. Selezionare Gruppo applicazione per Tipo, fare clic su Cerca identità e quindi su Cerca.
   b. Selezionare le identità fra quelle disponibili, e fare clic sul pulsante Sposta per ricollocarle nella casella Identità selezionate.

9. Se il tipo di criterio è di accesso, tutte le azioni, per impostazione predefinita, vengono selezionate per tutte le risorse. Per personalizzare tutto ciò, completare la configurazione dei criteri di accesso come segue:
   a. Selezionare una risorsa dall'elenco a discesa Aggiungi risorsa, e fare clic su Aggiungi.
      - Selezionare AppObject se le risorse di cui si deve configurare l'accesso in lettura o scrittura sono specifiche di CA User Activity Reporting Module.
      - Selezionare Utente ed Utente globale per accedere al pulsante Utenti sulla scheda Amministrazione, sottoscheda Gestione utenti e accessi.
      - Selezionare Gruppo utente e Gruppo utente globale per accedere ai pulsanti Gruppi nella scheda Amministrazione, sottoscheda Gestione utenti e accessi.
      - Selezionare Criterio per accedere ai pulsanti Criteri d'accesso, Cartelle EEM e Test dei criteri nella scheda Amministrazione, sottoscheda Gestione utenti e accessi.
      - Selezionare Calendario per accedere al pulsante Calendari nella scheda Amministrazione, sottoscheda Gestione utenti e accessi.
      - Selezionare iPoz per accedere ai pulsanti Criterio di password e Archivio utente nella scheda Amministrazione, sottoscheda Gestione utenti e accessi.
   b. Selezionare lettura per assegnare o negare l'accesso di visualizzazione, e scrittura per assegnare o negare l'accesso di modifica. Se non si seleziona nulla, verranno selezionate tutte le azioni.

      Nota: per assegnare o negare l'accesso di creazione, si deve definire un criterio di accesso a CALM e selezionarne singolarmente le risorse.
   c. Se necessario, aggiungere un filtro generico compatibile con le risorse selezionate.

10. Se il tipo di criterio è Elenco controllo di accesso, completare la relativa configurazione come segue:
    a. Selezionare una risorsa dall'elenco a discesa Aggiungi risorsa e fare clic sul pulsante Aggiungi (+).
    b. Selezionare lettura, scrittura o entrambe come Azioni.
    c. Fare clic sul pulsante Modifica filtri per aprire il modulo di filtro. Creare un filtro per la risorsa associata selezionando o inserendo dei valori per Sinistra (tipo o valore), Operatore (tipo o valore) e Destra (tipo o valore).
    d. Se il filtro contiene un nome di risorsa come valore, selezionare la casella denominata Tratta i nomi di risorsa come normali espressioni. In alternativa, non selezionare tale casella.

    Importante: definire un criterio per ogni combinazione di risorsa e filtri.

11. Se il tipo di criterio è Elenco controllo di accesso identità, completare la relativa configurazione come segue:
    a. Come Tipo, selezionare una delle opzioni visualizzate. Ad esempio, selezionare Gruppo applicazione, fare clic sul collegamento Cerca identità, e quindi sul pulsante Cerca per visualizzare i membri del tipo selezionato.
    b. Selezionare le identità e fare clic sul pulsante di spostamento per popolare il pannello Identità selezionate.
    c. Per ogni identità selezionata, specificare lettura, scrittura o entrambe.

       Le azioni specifiche dell'identità si applicano a tutte le risorse selezionate. Cioè, una data identità può visualizzare, visualizzare e modificare o semplicemente modificare tutte le risorse selezionate.
    d. Aggiungere le risorse a cui consentire o negare le azioni specifiche di un'identità.
12. Controllare le caselle di controllo e selezionare quelle applicabili:
    - Selezionare Negazione esplicita per modificare un criterio che garantisca l'accesso in uno che lo neghi
    - Selezionare Disabilitato per disattivare temporaneamente questo criterio, a patto che sia nuovo.
    - Selezionare Distribuzione preliminare, Assegna etichette ed aggiungere delle etichette, a patto di utilizzare questo criterio per motivi di verifica e di voler suddividere i criteri in categorie utilizzando etichette personalizzate.
13. Fare clic su Salva e quindi su Chiudi, nel riquadro di sinistra.

Ulteriori informazioni:

Passaggio 3: creazione del criterio di accesso al sistema Win-Admin (a pagina 119)

Creazione di un criterio basato su un criterio esistente

È possibile creare un nuovo criterio di accesso copiandone uno esistente e modificando la copia. Con questa procedura si risparmia il tempo che occorrerebbe per duplicare manualmente le specifiche di un criterio esistente che richieda soltanto lievi modifiche per soddisfare i requisiti correnti.

Soltanto gli amministratori possono creare, modificare, eliminare o visualizzare i criteri di accesso.

Per creare un criterio basato su un criterio esistente

1. Fare clic sulla scheda Amministrazione e sulla sottoscheda Gestione utenti e accessi.
2. Fare clic su Criteri di accesso.
3. Selezionare CALM o Criteri di scoping, a seconda del tipo di criterio che si vuole utilizzare come modello.
4. Fare clic sul collegamento del nome per aprire il criterio da copiare.
5. Fare clic su Salva con nome.

   Viene visualizzata la finestra di dialogo Prompt utente Explorer.
6. Inserire il nome del nuovo criterio che si deve basare sul criterio aperto e fare clic su OK.
7. Apportare le modifiche necessarie.

   Ad esempio, sostituire l'identità copiata con il nome del ruolo (gruppo utente dell'applicazione definito dall'utente) cui si applica questo criterio. Si potrebbero modificare le azioni permesse sulle risorse copiate. Fare clic su Filtri per specificare un filtro aggiuntivo per il nuovo ruolo.

8. Fare clic su Salva, quindi su Chiudi.
9. Verificare la definizione del nuovo criterio.
   a. Riselezionare il tipo di criterio per visualizzare tutti i criteri.
   b. Confrontare il criterio nuovo con quello originale e verificare che siano presenti tutte le modifiche previste.
   c. Fare clic su Chiudi.
10. Testare il criterio.

Ulteriori informazioni:

Passaggio 5: creazione di un criterio basato sul criterio di visualizzazione-modifica rapporti per analisti (a pagina 134)

Verifica di un nuovo criterio

È possibile verificare se la sintassi di un nuovo criterio è corretta grazie alla funzione Testa criterio. La funzione Testa criterio consente di avviare query ad hoc a fronte dei criteri di accesso impostati. Un'autorizzazione può essere considerata come una richiesta: "{Identità} può eseguire {azione} a fronte della risorsa di tipo {classe risorsa} e di nome {risorsa} [con i seguenti attributi}] [alle {ora specificata}]?" Il risultato ALLOW indica che l'identità inserita può eseguire l'azione specificata sulla risorsa specificata con gli attributi specificati e all'ora specificata.

Prima di iniziare, è necessario avere a portata di mano il proprio criterio.

Per verificare un criterio

1. Fare clic sulla scheda Amministrazione e sulla sottoscheda Gestione utenti e accessi.
2. Fare clic su Testa criterio.

   Viene visualizzata la pagina Parametri controllo autorizzazione.
3. Se nel criterio che si prevede di controllare è selezionata la pre-distribuzione e sono presenti etichette aggiunte, selezionare la casella di controllo che indica l'intenzione di includere i criteri di pre-distribuzione e di aggiungere le etichette associate.
4. Completare i campi di immissione. Se il criterio include dei filtri, specificarli nell'ordine di comparsa nel criterio.
5. Fare clic su Avvia controllo autorizzazione.
6. Osservare il risultato e procedere in uno dei modi seguenti:
   - Se il risultato è ALLOW, accedere a CA User Activity Reporting Module come utente specificato come identità in questo nuovo criterio e verificare efficienza, scopo e copertura prima di metterlo ad uso di produzione.
   - Se il risultato è DENY, verificare le voci della query. Se sono corrette, ritornare al criterio e apportare le correzioni necessarie.

Creazione di un criterio per un gruppo utente dinamico

Un *gruppo utenti dinamico* è composto da utenti globali che condividono uno o più attributi comuni. Un gruppo utente dinamico viene creato tramite uno speciale criterio in cui il nome della risorsa è il nome del gruppo utente dinamico e l'appartenenza è basata su un set di filtri configurati in base agli attributi di utente e gruppo.

È possibile creare un gruppo dinamico composto da utenti, gruppi applicazione, gruppi globali o gruppi dinamici. Ad esempio, è possibile creare un gruppo dinamico di gruppi globali o gruppi applicazione basato su nome, descrizione o appartenenza a un gruppo. Altrimenti, si può creare un gruppo dinamico di utenti con ruoli diversi basati su un attributo comune nel profilo utente globale, ad esempio:

- Professione
- Reparto o ufficio
- Città, Stato o Paese

Soltanto gli amministratori sono autorizzati a creare criteri per i gruppi utente dinamici.

Per creare un criterio per un gruppo utente dinamico

1. Fare clic sulla scheda Amministrazione e sulla sottoscheda Gestione utenti e accessi.
2. Fare clic su Criteri di accesso.
3. Fare clic su Nuovo criterio gruppo dinamico.

   Viene visualizzata la pagina Nuovo criterio gruppo dinamico.
4. Specificare nel campo Nome un nome gruppo che indichi una caratteristica comune di questo gruppo di utenti. (Facoltativo) Immettere una descrizione.
5. Selezionare un tipo di criterio. Il criterio predefinito è Criterio di accesso.

6. Selezionare le identità come segue:
   a. In Tipo, selezionare Utente, Gruppo applicazione, Gruppo globale o Gruppo dinamico e fare clic su Cerca identità.
   b. In Attributo, Operatore e Valore, inserire l'espressione di impostazione dei criteri di appartenenza a questo gruppo e fare clic su Cerca.

      Ad esempio, se si seleziona Utente, è possibile specificare una professione come manager e fare clic su Cerca per trovare tutti gli utenti con questa professione.
   c. Selezionare tra le identità visualizzate quelle che faranno parte del gruppo dinamico e fare clic sulla freccia Sposta per trasferire le selezioni nella casella Identità selezionate.
7. In Azioni, selezionare appartenenza.
8. Nel campo Aggiungi risorsa, inserire il valore immesso nel campo Nome e fare clic sul pulsante Aggiungi. Questo indica che le identità selezionate appartengono alla risorsa del gruppo dinamico appena creato.
9. (Facoltativo) Aggiungere altri filtri.
10. Fare clic su Salva.
11. Fare clic sul link Criteri gruppo utente dinamico e controllare il nuovo gruppo utente dinamico appena creato. Ad esempio:

Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
Non-Administrators	SafeDynamicUserGroup	Concessione esplicita	ug:Auditor ug:ResourceAccessAnalyst ug:CALM-Analyst ug:Analyst	belong	Non-Administrators
QA Group	SafeDynamicUserGroup	Concessione esplicita	User1 User3 User2	belong	QA Group
Security Offcers	SafeDynamicUserGroup	Concessione esplicita	Administrator1 User3	belong	Security Offcers

Creazione di un filtro di accesso

È possibile creare un filtro di accesso per limitare l'accesso ai dati di registro che soddisfano i criteri del filtro. Per impostazione predefinita, tutti gli utenti delle applicazioni CA User Activity Reporting Module hanno accesso query ai dati del registro eventi memorizzati negli archivi registro eventi del server CA User Activity Reporting Module attivo, nei server peer di una federazione a coppie o nei server discendenti in una federazione gerarchica.

È possibile limitare l'accesso all'archivio registro eventi di uno o più server CA User Activity Reporting Module specifici creando un filtro di accesso ai dati. Il filtro di accesso può essere applicato a un individuo o a un gruppo.

Per creare un filtro di accesso per un ruolo definito dall'utente

1. Fare clic sulla scheda Amministrazione e sulla sottoscheda Gestione utenti e accessi.
2. Fare clic su Nuovo filtro di accesso.

   Viene visualizzata la procedura guidata progettazione filtro di accesso,
3. Nella sezione Dettagli, specificare il nome e la descrizione del filtro.
4. Fare clic su Identità. Selezionare un tipo di identità, fare clic sul pulsante di ricerca per visualizzare le identità disponibili e utilizzare il controllo pilota per selezionare quelle a cui applicare questo filtro di accesso.

   Ad esempio, selezionare il gruppo applicazione creato a questo scopo.

5. Impostare i filtri di accesso.
   a. Fare clic su Filtri di accesso.
   b. Fare clic sul pulsante Nuovo filtro evento.

   c. Aggiungere una o più espressioni che definiscano il filtro di accesso.
   d. Fare clic su Salva e chiudi.

   Viene visualizzato il filtro di accesso creato.
6. Fare clic su Chiudi.

Ulteriori informazioni:

Passaggio 4: creazione di filtri di accesso ai dati Win-Admin (a pagina 123)
Creazione di un gruppo utente delle applicazioni (ruolo) (a pagina 87)

Gestione di account utente e criteri di accesso

In qualità di amministratore, è possibile eseguire le seguenti attività di gestione relative ad account utente e criteri di accesso:

- Bloccare un account utente in modo che tale utente non possa più accedere a CA User Activity Reporting Module;
- Sbloccare gli account utente che erano stati bloccati, se il criterio delle password non permette ad alcun utente di sbloccare un account utente bloccato;
- Aggiungere nuovi account utente;
- Modificare account utente esistenti;
- Bloccare o eliminare account utente che appartengono a persone cui non occorre più l'accesso a CA User Activity Reporting Module;
- Modificare criteri di accesso esistenti;
- Eliminare criteri di accesso che non sono più necessari;

- Creare, modificare o eliminare i criteri di delega;
- Creare, modificare o eliminare i filtri di accesso con i corrispondenti criteri di obbligo generati automaticamente;
- Creare un ruolo superiore dai ruoli esistenti con accesso limitato;
- Aggiungere un nuovo ruolo personalizzato e i criteri di accesso corrispondenti.

Creazione di un calendario

È possibile creare un nuovo calendario per meglio limitare l'accesso degli utenti in alcuni periodi di tempo. I calendari funzionano come parte dei criteri di accesso. Quando si definisce un calendario, è possibile includere o escludere blocchi temporali di ore, giorni della settimana o date.

Per creare un calendario

1. Fare clic sulla scheda Amministrazione, quindi su Gestione utenti e accessi e infine sul pulsante Calendari.

   Viene visualizzata la pagina Calendari.

2. Fare clic sull'icona Nuovo calendario in alto a sinistra dell'elenco di calendari.

   Viene visualizzato il riquadro dei dettagli Nuovo calendario.

3. Inserire un nome che specifichi il criterio di destinazione e fornisca una descrizione dell'uso previsto.
4. Utilizzare le icone del calendario per impostare le date di inizio e di fine del calendario.
5. Fare clic su Aggiungi inclusione blocco temporale o Aggiungi esclusione blocco temporale per creare periodi di eccezione nell'ambito del periodo di efficienza principale del calendario.
6. Fare clic su Salva, quindi su Chiudi.

Ulteriori informazioni:

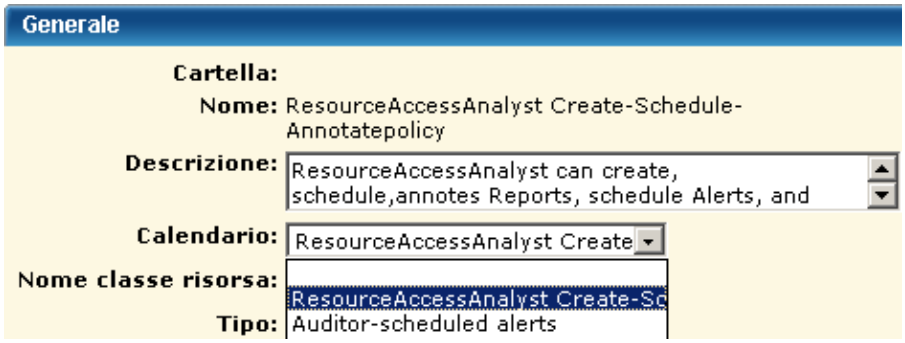
Aggiunta di un calendario a un criterio (a pagina 106)

Aggiunta di un calendario a un criterio

Al momento di creare un criterio, è possibile selezionare un calendario esistente che indichi quando le identità specifiche possono eseguire le azioni selezionate sulle risorse specifiche. Con un calendario è possibile definire le date di inizio e di fine e blocchi temporali di ore o giorni della settimana.

Per aggiungere un calendario a un criterio

1. Fare clic sulla scheda Amministrazione e sulla sottoscheda Gestione utenti e accessi.
2. Aprire il criterio a cui si applica il calendario.
   a. Fare clic su Criteri di accesso.
   b. Selezionare il tipo di criterio.
   c. Selezionare il criterio.
3. Aprire l'elenco a discesa del calendario e selezionare quello creato per questo criterio.



4. Fare clic su Salva per salvare il calendario aggiunto a un criterio esistente.

Ulteriori informazioni:

Creazione di un calendario (a pagina 105)

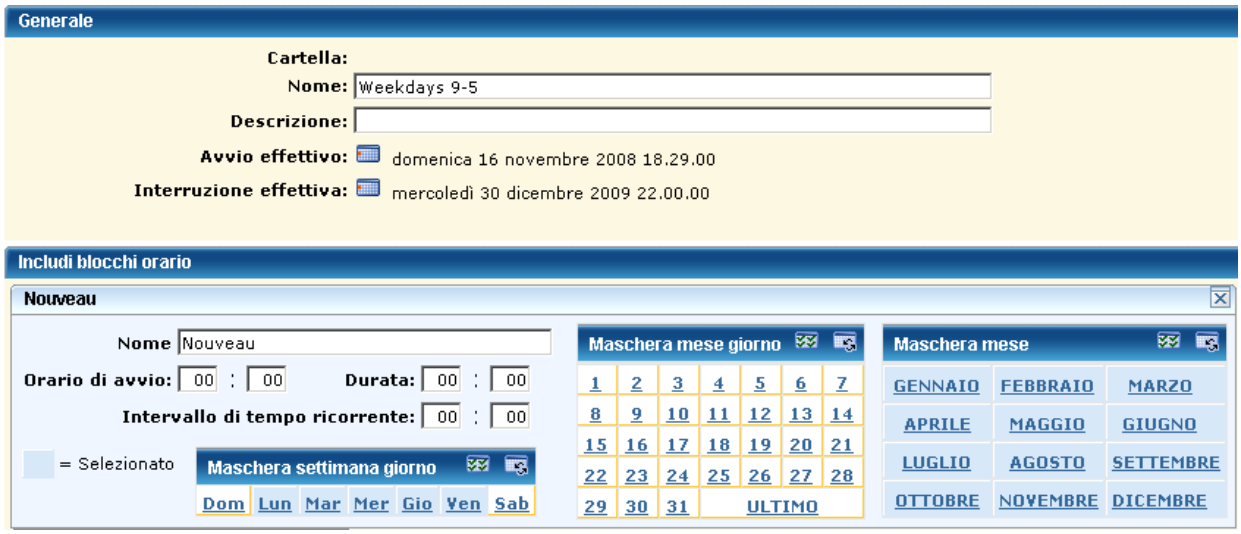
Esempio: limitazione dell'accesso ai giorni lavorativi

È possibile limitare l'ora o i giorni della settimana in cui un dato gruppo di utenti può accedere a CA User Activity Reporting Module tramite la creazione di un calendario che stabilisca l'ora in cui garantire l'accesso, la creazione di un ruolo personalizzato, la creazione di un nuovo criterio basato sul criterio di accesso a CA User Activity Reporting Module e l'assegnazione del calendario e del ruolo personalizzato a questo criterio.

Esempio: limitazione dell'accesso a CA User Activity Reporting Module per i revisori esterni ai giorni feriali

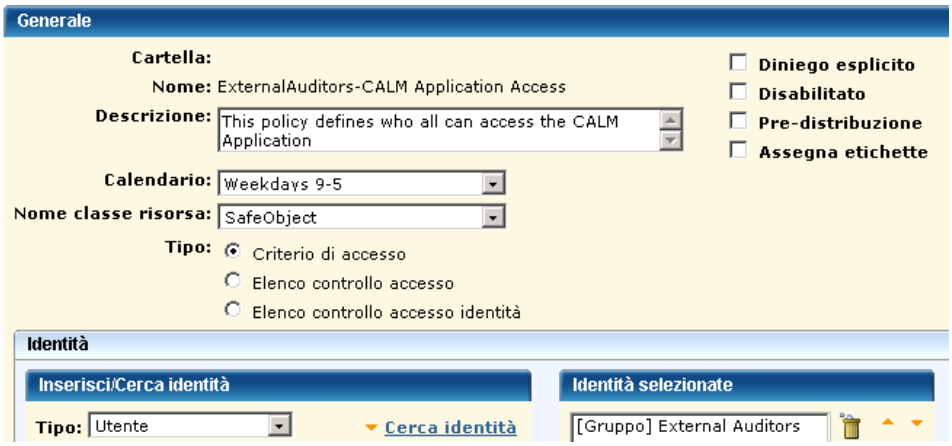
Per limitare l'accesso di alcuni gruppi a CA User Activity Reporting Module ai giorni lavorativi, creare un calendario dei giorni feriali e aggiungerlo ai criteri che garantiscono un accesso specifico ai revisori.

Ad esempio, se si vuole limitare alle ore lavorative l'accesso dei revisori esterni a CA User Activity Reporting Module, creare un calendario che specifichi i giorni feriali, da lunedì a venerdì, dalle 9.00 alle 17.00, per tutti i mesi dell'anno.



Creare un ruolo per i revisori esterni.

Aprire il criterio di scoping per l'accesso all'applicazione CALM e salvarlo come Accesso all'applicazione CALM-Revisori esterni. Poi, selezionare il calendario dei giorni feriali con impostate le ore dalle 9.00 alle 17.00 e selezionare il gruppo utenti Revisori esterni come identità.



Importante: utilizzare la funzione Calendario solo con i criteri che garantiscono l'accesso. Non utilizzarla con i criteri che negano l'accesso.

Ulteriori informazioni:

Creazione di un calendario (a pagina 105)
Creazione di un gruppo utente delle applicazioni (ruolo) (a pagina 87)
Creazione di un criterio basato su un criterio esistente (a pagina 98)
Aggiunta di un calendario a un criterio (a pagina 106)

Esportazione dei criteri di accesso

È possibile esportare in qualunque momento qualsiasi tipo di criterio selezionato, che si tratti di criteri predefiniti o personalizzati. L'esportazione dei criteri è un buon metodo per mantenere un backup aggiornato.

L'esportazione crea un file XML per ogni criterio selezionato, in cui i file XML sono compressi in un file chiamato CAELM[1].xml.gz.

Per esportare i criteri di accesso

1. Fare clic sulla scheda Amministrazione e sulla sottoscheda Gestione utenti e accessi.
2. Fare clic su Criteri di accesso.
3. Selezionare il tipo di criterio di accesso da esportare e fare clic su Esporta.

   Viene visualizzata la finestra di dialogo Download del file.
4. Fare clic su Salva e salvare il file con un nome univoco.
5. Fare clic su Chiudi.

Ulteriori informazioni:

Eseguire il backup di tutti i criteri di accesso (a pagina 61)

Eliminazione di un criterio personalizzato

È possibile eliminare un criterio personalizzato per uno qualsiasi dei motivi seguenti:

- È stato salvato con un nome diverso e non si prevede di apportare ulteriori modifiche, quindi è necessario eliminare il duplicato.
- Non si appartiene più attivamente alle identità definite dal criterio, che quindi non è più usato.

Importante: assicurarsi di non eliminare i criteri predefiniti. Se questo dovesse accadere, è possibile ripristinarli se è stato esportato un backup.

Per eliminare un criterio personalizzato

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Gestione utenti e accessi.
2. Fare clic su Criteri di accesso.

3. Selezionare CALM o Criteri di scoping, a seconda del tipo di criterio da eliminare.
4. Fare clic sul nome del criterio da eliminare.
5. Fare clic su Elimina.
6. Fare clic su OK per confermare l'eliminazione.

Eliminazione di filtri di accesso e criteri di obbligo

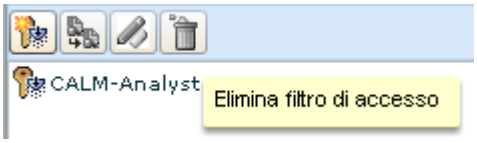
È possibile eliminare un filtro di accesso e il criterio di obbligo generato dal filtro per rimuovere la limitazione di accesso ai dati.

Non eliminare il criterio di obbligo generato dal filtro dai criteri di accesso.

Per eliminare un filtro di accesso e il relativo criterio di obbligo

1. Fare clic sulla scheda Amministrazione, quindi su Gestione utenti e accessi.

   Viene visualizzato l'Elenco filtri di accesso nella parte superiore del riquadro a sinistra.
2. Selezionare il filtro da eliminare e fare clic sul pulsante Elimina filtro di accesso.

   Viene visualizzato il messaggio di avviso di conferma dell'eliminazione del filtro di accesso.
3. Fare clic su Sì per rimuovere il filtro di accesso selezionato e il criterio di obbligo associato.

Esempio: consentire a chi non è amministratore di gestire gli archivi

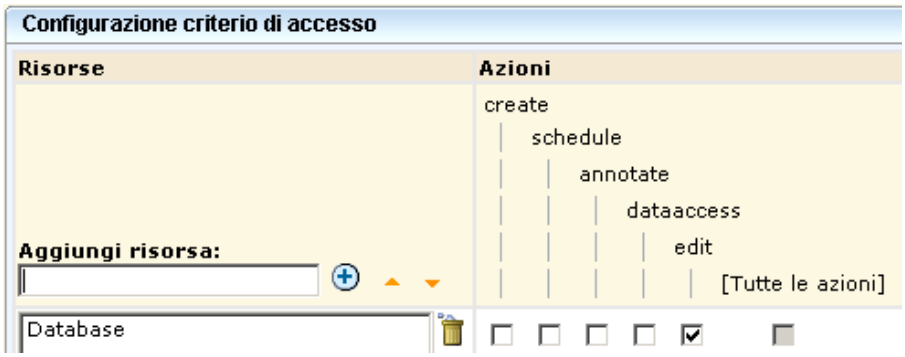
Si supponga di voler consentire a un gruppo di non amministratori di gestire l'archiviazione automatica. È possibile creare un gruppo di nome ArchiveAdministrator, un criterio CALM che consente azioni di modifica sul database delle risorse. Questo permette l'accesso in lettura al catalogo dell'archivio del database per l'esecuzione di query, l'accesso in scrittura al catalogo dell'archivio per la ricatalogazione e la possibilità di sfruttare l'utility LMArchive per l'archiviazione manuale o lo script shell restore-ca-elm per il ripristino dei database archiviati automaticamente.

Per consentire a chi non è amministratore di gestire l'archiviazione

1. Creare un ruolo chiamato ArchiveAdministrator.
   a. Selezionare la scheda Amministrazione, quindi la sottoscheda Gestione utenti e accessi.
   b. Selezionare Gruppi.
   c. Fare clic su Nuovo gruppo dell'applicazione.
   d. Specificare ArchiveAdministrator come nome.
   e. Fare clic su Salva.

      Viene creato il gruppo, o ruolo, applicazione ArchiveAdministrator.
   f. Fare clic su Chiudi.

2. Creare un criterio CALM che consenta l'accesso in modifica alla risorsa database.
   a. Fare clic su Criteri di accesso.
   b. Fare clic su Nuovo criterio di accesso per creare un nuovo criterio CALM.
   c. Digitare Criterio ArchiveAdministrator nel campo Nome.
   d. Nella descrizione, inserire: ArchiveAdministrator può avviare l'utility LMArchive e lo script shell restore-ca-elm.
   e. In Identità, selezionare Gruppo applicazione come Tipo; quindi, fare clic su Cerca identità e infine su Cerca.
   f. Selezionare ArchiveAdministrator e fare clic sulla freccia Sposta.
   g. Digitare Database in Aggiungi risorsa e fare clic su Aggiungi.
   h. Impostare la modifica ad Azione.



   i. Fare clic su Salva. Fare clic su Chiudi.

3. Testare il criterio e verificare che il risultato sia ALLOW.

Risultato	Criterio	Delegante	Identità	Classe risorsa	Risorsa	Azione
CONSENTI	test		ArchiveAdministrator	CALM	Database	edit

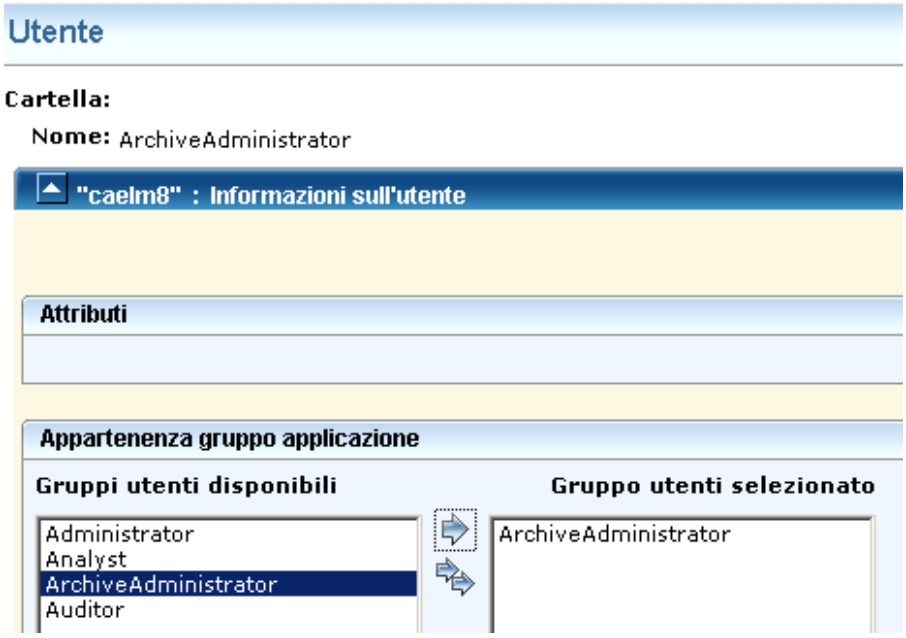
4. Concedere al ruolo ArchiveAdministrator l'autorizzazione ad accedere a CA User Activity Reporting Module.
   a. Fare clic su CALM in Criteri di accesso.
   b. Selezionare Accesso all'applicazione CALM.
   c. In Identità, cercare il gruppo applicazione ArchiveAdministrator e trasferirlo in Identità selezionate.

   d. Fare clic su Salva. Fare clic su Chiudi. Fare clic su Chiudi.

      La scheda Gestione utenti e accessi viene visualizzata assieme ai pulsanti nel riquadro sinistro.

5. Assegnare il ruolo ArchiveAdministrator a uno o più utenti.
   a. Fare clic su Utenti.
   b. Inserire il nome di una persona a cui assegnare questo ruolo come Valore in Ricerca utenti e fare clic su Vai a.

      Il nome utente selezionato appare sotto la cartella Utenti.
   c. Scegliere il link per l'utente selezionato.
   d. Fare clic su Aggiungi dettagli utente applicazione.
   e. Spostare ArchiveAdministrator nell'elenco Gruppi utente selezionati.



   f. Fare clic su Salva. Fare clic su Chiudi.
   g. Ripetere l'operazione per tutti gli utenti da assegnare a questo ruolo.
   h. Fare clic su Chiudi.

6. (Facoltativo) Ricontrollare i risultati da CA User Activity Reporting Module.
   a. Fare clic su Disconnessione per disconnettersi come amministratore.
   b. Accedere come utente al quale sia stato assegnato il ruolo di ArchiveAdministrator.
   c. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Raccolta registri.
   d. Selezionare Archivia query di catalogo.
   e. Controllare di utilizzare i pulsanti Query e Ricataloga.
7. (Facoltativo) Avviare lo script restore-ca-elm con le credenziali dell'utente definito con il ruolo ArchiveAdministrator per verificare che i criteri funzionino come previsto.

Ulteriori informazioni:

Ripristino dei file archiviati automaticamente (a pagina 207)

Limitazione dell'accesso ai dati per un utente: scenario Win-Admin

È possibile limitare i rapporti visualizzati dall'utente a quelli contraddistinti da un tag specifico. Questi dati possono essere limitati a quelli generati dalle origini evento specificate. La limitazione dell'accesso ai rapporti con un determinato tag viene definita grazie a un criterio di accesso, mentre la limitazione dell'accesso ai dati degli eventi restituiti da un particolare server CA User Activity Reporting Module viene definita con un filtro di accesso. Dopo aver definito un filtro di accesso, l'assegnazione del ruolo è facoltativa. Questo significa che è possibile creare un nuovo utente, non assegnare alcun ruolo e limitare l'accesso ai dati per quell'utente con un filtro di accesso.

Considerare l'esempio dell'azienda ABC con quattro centri dati negli Stati Uniti. L'amministratore vuole consentire all'amministratore Windows della regione di Houston l'accesso in lettura agli eventi Windows elaborati dal controller di dominio nell'area di Houston. Gli eventi Windows elaborati dal server CA User Activity Reporting Module installato sul controller di dominio di Houston vengono inviati dalle origini in cui il nome host inizia con la stringa ABC-HOU-WDC.

Questo esempio mostra come creare un utente chiamato Win-Admin e come assicurarsi che tale utente possa visualizzare soltanto i rapporti con un tag di accesso al sistema e che i dati di questi rapporti siano limitati agli eventi delle origini evento con nomi host che iniziano con la convenzione di denominazione conosciuta.

L'esempio fornisce dettagli per ognuno dei passaggi seguenti:

1. Creare il nuovo utente Win-Admin.
2. A Win-Admin viene concesso l'accesso di base a CA User Activity Reporting Module. Aggiungere questa identità al criterio di accesso all'applicazione CALM.
3. Restringere l'accesso ai rapporti per Win-Admin a quelli con il tag di accesso al sistema. Creare un criterio di scoping con accesso in lettura ad AppObject con filtri che specifichino la cartella EEM in cui sono memorizzati i rapporti e specificare che il calmTag corrisponde all'accesso al sistema. Testare il criterio.
4. Limitare i dati che Win-Admin può visualizzare a quelli generati dal controller di dominio nella sua regione. Creare un filtro di accesso, chiamato filtro di accesso ai dati Win-Admin, che limiti i dati di query e rapporti che Win-Admin può visualizzare agli eventi Windows provenienti da origini evento con nome host che inizia con ABC-HOU-WDC.
5. Accedere a CA User Activity Reporting Module come utente Win-Admin e valutare l'accesso consentito dai criteri.
6. Se l'accesso è troppo limitato perché l'utente possa eseguire le attività previste, estendere l'accesso tramite criteri aggiuntivi.

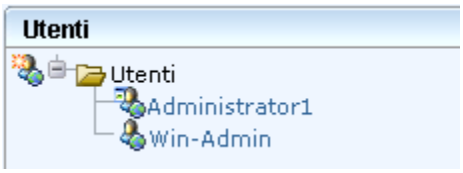
Passaggio 1: creazione dell'utente Win-Admin

È possibile creare un utente privo di ruolo (gruppo applicazione) se si specifica l'accesso ai dati con un filtro di accesso.

In questo modo, il primo passaggio del procedimento completo per la limitazione dell'accesso ai dati è la creazione dell'utente.

È necessario creare un utente soltanto se l'account dell'utente globale non è disponibile per l'importazione da una directory esterna. Quando si crea un account di questo tipo, non aggiungere dettagli sull'utente dell'applicazione. In questo scenario di esempio, il nome utente sarà Win-Admin.

Se si conduce una ricerca di utenti, il nuovo nome viene visualizzato nell'elenco.



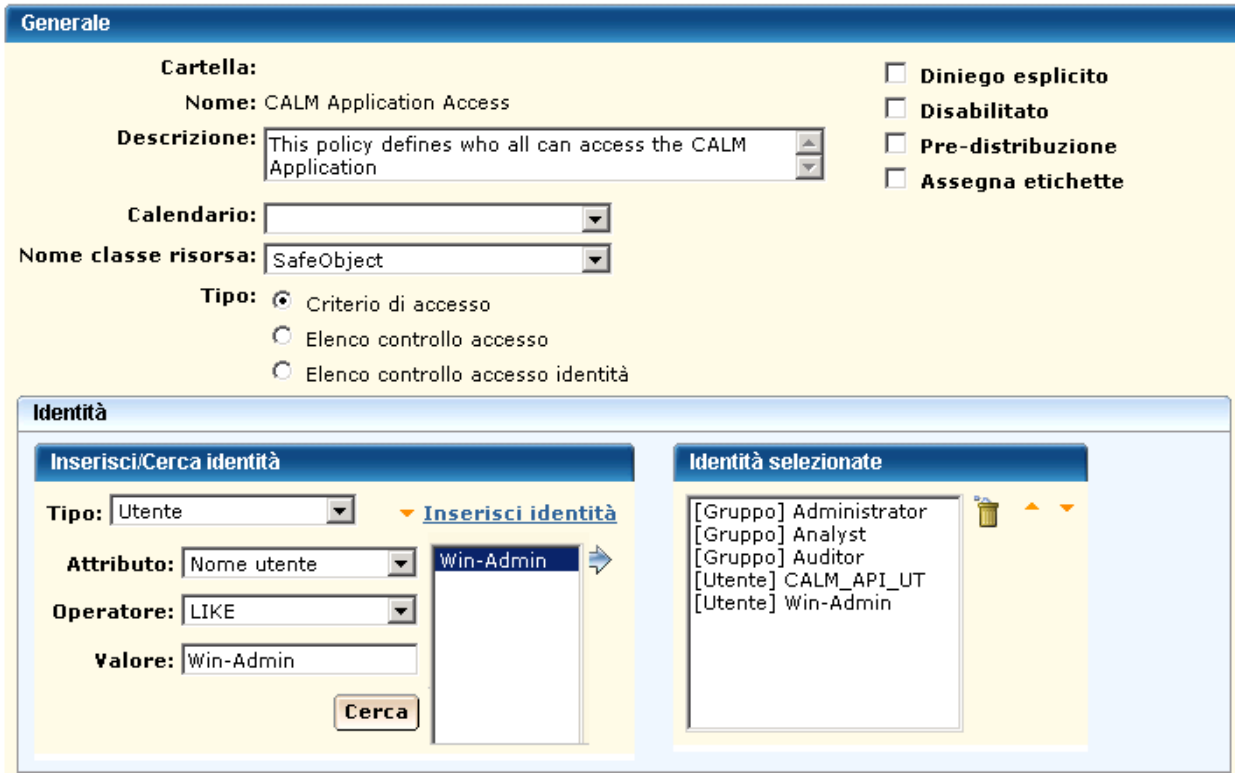
Ulteriori informazioni:

Creazione di un utente globale (a pagina 39)

Passaggio 2: aggiunta di Win-Admin al criterio di accesso all'applicazione di CALM

Il secondo passaggio della limitazione dell'accesso ai dati per un utente chiamato Win-Admin è quello di garantire a questa identità l'accesso all'applicazione CA User Activity Reporting Module.

Aggiungere il nuovo utente al criterio di accesso all'applicazione CALM. La procedura è identica a quella che consente a un nuovo ruolo di accedere a CA User Activity Reporting Module, ad eccezione di quando si cercano le identità, nel qual caso occorre specificare il Tipo come Utente.



Ulteriori informazioni:

Come garantire l'accesso ruolo personalizzato a CA User Activity Reporting Module (a pagina 88)

Passaggio 3: creazione del criterio di accesso al sistema Win-Admin

Il passaggio 2 garantisce l'accesso all'applicazione CA User Activity Reporting Module.

Il passaggio 3, invece, garantisce o esamina l'accesso all'applicazione CA User Activity Reporting Module dopo il logon. Su scala più ampia, si può garantire l'accesso di sola lettura o l'accesso in lettura e scrittura alle identità specificate.

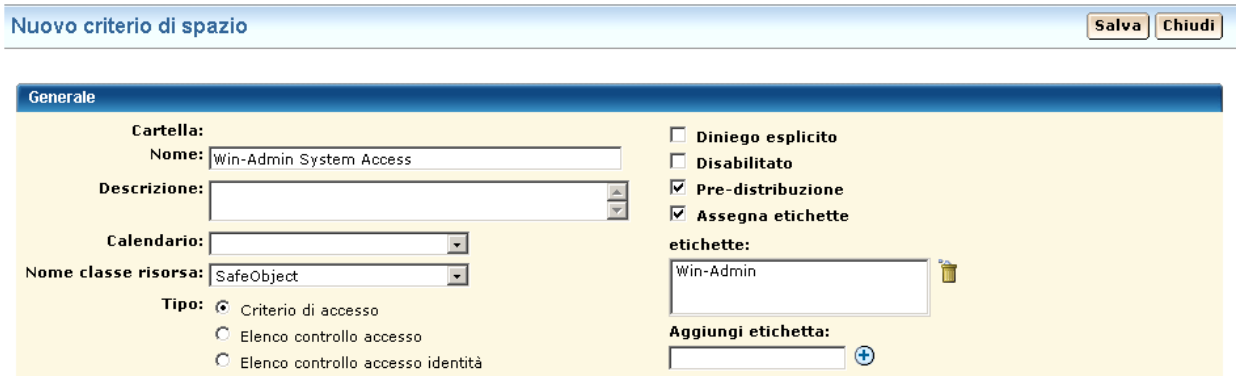
La selezione del tipo di criterio determina la granularità con cui è possibile specificare le azioni consentite.

- I criteri di accesso permettono l'esecuzione delle azioni scelte sulle risorse selezionate applicabili.
- I criteri degli elenchi di controllo di accesso consentono di specificare quali azioni sono consentite su ogni risorsa aggiunta.
- I criteri degli elenchi di controllo di accesso consentono di specificare quali azioni sulle risorse applicabili sono permesse da ogni identità.

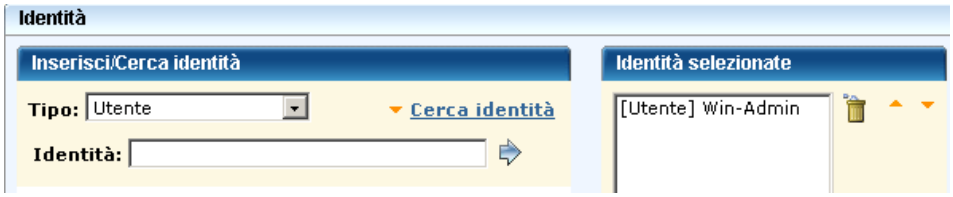
Si può consentire l'accesso limitato a una risorsa creando un filtro che specifichi la cartella EEM per quella risorsa e poi indicando in tale cartella le limitazioni.

Questo esempio mostra come limitare in generale l'accesso ad accesso in sola lettura, con ulteriori restrizioni per una funzione specifica. In particolare, il passaggio 3 limita la visualizzazione dei rapporti di accesso al sistema per l'utente Win-Admin. L'esempio seguente mostra come creare un criterio di scoping chiamato Accesso al sistema Win-Admin che garantisca l'accesso in lettura a SafeObject e AppObject e indichi i filtri che limitano l'accesso ai rapporti dotati del tag di accesso al sistema. Mostra anche come testare il criterio e, dopo la verifica, come rimuovere le impostazioni di distribuzione preliminare.

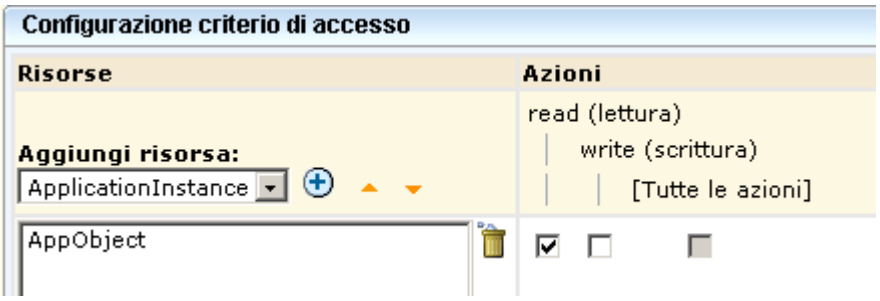
L'area Generale di un criterio di scoping, creato per impostare l'accesso all'applicazione ad accesso di sola lettura o di lettura e scrittura, indica SafeObject come nome della classe della risorsa. L'esempio seguente mostra il nome del criterio di accesso al sistema Win-Admin. Si consiglia di selezionare Distribuzione preliminare per un nuovo criterio fino a quando tale criterio sarà stato testato e sarà stato dimostrato che è pronto all'utilizzo in un ambiente di produzione.



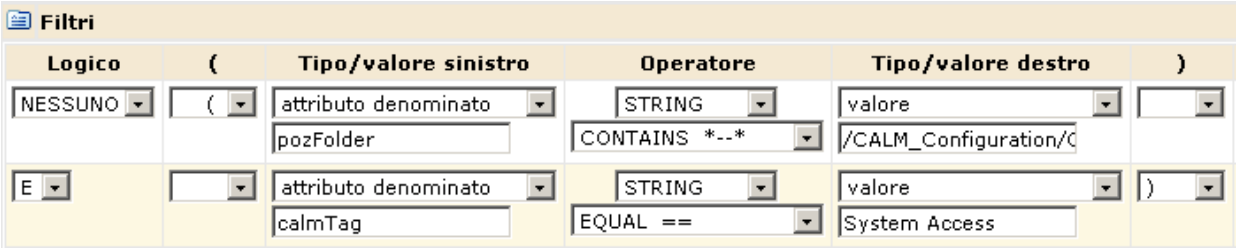
È possibile garantire l'accesso a utenti o gruppi. In questo esempio, l'accesso è garantito al nuovo utente Win-Admin.



Il criterio "di massimo livello" creato per CA User Activity Reporting Module è il criterio di accesso a CALM, dove l'istanza dell'applicazione è CAELM. Questo criterio di scoping è volto a specificare che l'azione di lettura è concessa sugli oggetti applicazione, AppObject, con riferimento a tutte le funzioni dell'applicazione.

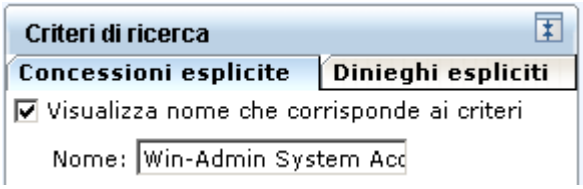


È possibile limitare ulteriormente l'azione specifica consentita su tutti gli oggetti definendo dei filtri. I filtri vengono spesso definiti a coppie: il primo filtro specifica la cartella CA EEM in cui vengono archiviati i dati relativi a una precisa funzione, mentre il secondo indica una limitazione sugli oggetti in quella posizione. Nell'esempio seguente, il primo filtro limita l'accesso alla cartella CA EEM in cui è archiviata la risorsa dei rapporti. In particolare, specifica che la cartella pozFolder contiene /CALM_Configuration/Content/Reports. Il secondo filtro limita l'accesso ai rapporti con il tag di accesso al sistema specificando che il calmTag equivale all'accesso al sistema.

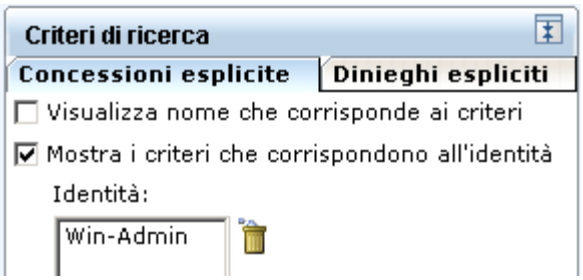


Dopo aver salvato un criterio, è possibile cercarlo per esaminarlo. I criteri possono essere cercati per nome, identità o risorsa. È possibile inserire un valore parziale o anche criteri multipli. Seguono alcuni esempi per questo scenario.

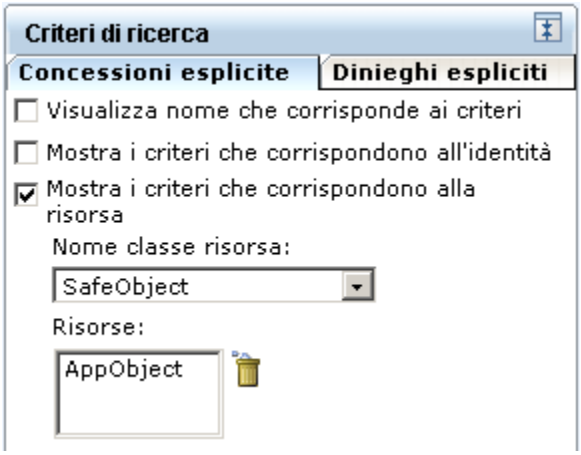
La ricerca in base al nome completo visualizza soltanto il criterio desiderato.



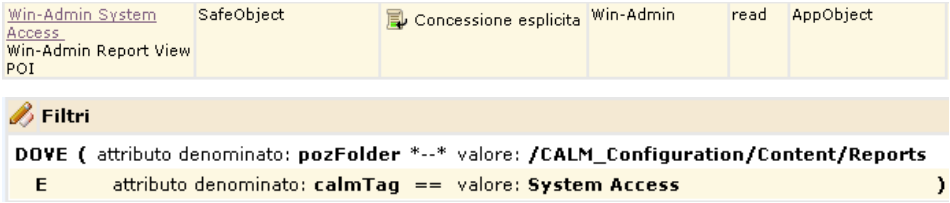
La ricerca in base all'identità visualizza tutti i criteri applicati a tale identità, inclusi quelli applicati a tutte le identità.



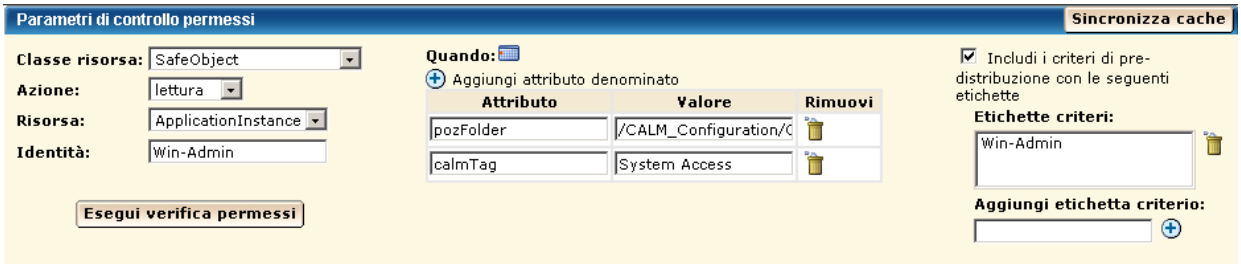
La ricerca in base alla risorsa, solo se la risorsa è AppObject, visualizza tutti i criteri forniti dal sistema o personalizzati che garantiscono accesso in lettura o in lettura e scrittura a un'identità.



Quando il criterio personalizzato che si sta cercando appare nella tabella dei criteri, esaminarne i valori, filtri compresi. Se si nota qualsiasi cosa richieda una correzione, è possibile fare clic sul link del nome per visualizzare nuovamente il criterio e modificarlo.



È consigliabile testare tutti i nuovi criteri. Assicurarsi di inserire le coppie attributo/valore nell'ordine in cui sono stati inseriti i filtri, con l'attributo di livello massimo per primo.



Verificare che il risultato sia ALLOW.

Risultati del controllo permessi — Cancella tutto

☐ Visualizza informazioni su debug ☑ Visualizza obblighi

Orario del controllo	Etichette di pre-distribuzione	Risultato	Criterio	Delegante	Identità	Classe risorsa	Risorsa	Azione	Quando	Attributi denominati	
										Nome	Valore
lunedì 28 settembre 2009 20.07.53	Win-Admin	CONSENTI	CALM Application Access		Win-Admin	SafeObject	ApplicationInstance	read		pozFolder	/CALM_Configuration/Content/Reports
										calmTag	System Access

Dopo averlo verificato, deselezionare l'impostazione di distribuzione preliminare del criterio. In caso contrario, non sarà possibile accedere come Win-Admin per valutare cosa può fare l'utente.

Generale

Cartella:

Nome: Win-Admin System Access

Descrizione:

☐ Diniego esplicito
☐ Disabilitato
☐ Pre-distribuzione
☐ Assegna etichette

Ulteriori informazioni:

Verifica di un nuovo criterio (a pagina 100)

Passaggio 4: creazione di filtri di accesso ai dati Win-Admin

Con il passaggio 3 si limita la visualizzazione di rapporti di accesso al sistema da parte dell'utente Win-Admin. Questo livello di accesso consente all'utente Win-Admin di visualizzare i rapporti di accesso al sistema in tutte e quattro le zone dell'azienda ABC.

Con il passaggio 4 si crea un filtro di accesso per limitare i dati visualizzabili dall'utente Win-Admin ai rapporti di accesso al sistema per il controllo di dominio Houston.

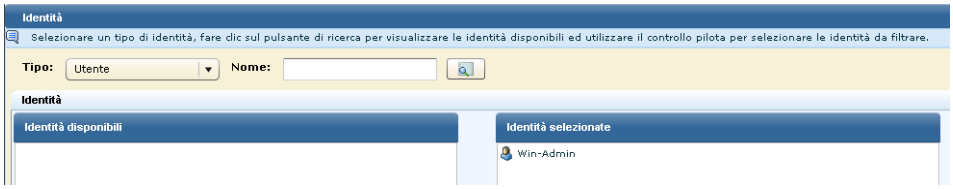
La creazione di un filtro di accesso ai dati inizia specificando il nome. Il nome utilizzato in questo esempio è Accesso dati Win-Admin.

Access Filter Details

Immettere un nome e una descrizione per il filtro.

Nome: Win-Admin Data Access

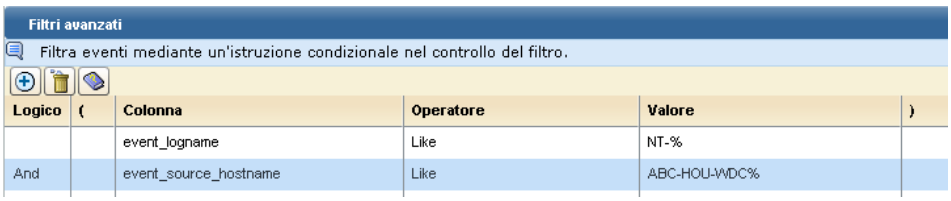
Occorre specificare le identità alle quali viene applicato il filtro di accesso nell'area Identità. Un filtro può essere applicato a utenti o a gruppi. In questo esempio, il filtro di accesso verrà applicato soltanto all'utente Win-Admin.



Per i filtri di accesso, si definisce ogni condizione in termini del valore di una colonna CEG. I valori che seguono l'operatore LIKE possono contenere l'uno o l'altro dei seguenti caratteri jolly:

- _ (carattere di sottolineatura): rappresenta ogni singolo carattere.
- % (segno di percentuale): rappresenta una stringa che contiene un numero qualsiasi di caratteri.

Il primo filtro per questo esempio gode del vantaggio che tutti gli eventi Windows hanno prefisso NT-. Per limitare i dati agli eventi Windows, è possibile specificare che la colonna CEG event_logname deve contenere dati che includano la stringa NT-%. Per limitare ulteriormente gli eventi Windows a quelli provenienti da un controller di dominio specifico, questo esempio indica che event_source_hostname deve possedere dati che includano una stringa che utilizzi le convenzioni locali. Il valore ABC-HOU-WDC% è basato su una convenzione di denominazione di un nome contenente trattini e composto da abbreviazioni che indicano l'azienda, la regione e il prefisso del tipo di controller di dominio.



Logico	(	Colonna	Operatore	Valore	)
		event_logname	Like	NT-%	
And		event_source_hostname	Like	ABC-HOU-WDC%	

Nota: in assenza di origini evento con una convenzione di denominazione standardizzata, è possibile creare un elenco di valori chiave con event_source_hostnames e utilizzare il nome dell'elenco come valore.

Quando sono presenti soltanto due filtri e l'operatore logico è AND, le parentesi non sono obbligatorie. Se invece si inserisce un'espressione complessa, come la seguente, le parentesi diventano obbligatorie.

```
(event_logname like NT-%
And event_source_hostname=ABC-%)
(event_logname like CALM-%
And event_source_hostname=XYZ-%)
```

Quando si salva un filtro di accesso ai dati, il relativo nome viene visualizzato nell'elenco dei filtri di accesso.

La ricerca di criteri corrispondenti al nome utente Win-Admin visualizza tre criteri per tutte le identità, oltre ad altri tre: il criterio di accesso all'applicazione CALM cui è stato aggiunto il Win-Admin, il criterio di accesso al sistema Win-Admin creato dal nulla e il criterio dei dati che viene aggiunto automaticamente quando si definisce un filtro di accesso. Il criterio dei dati viene elencato per primo nell'immagine seguente. Può essere visualizzato anche in Criteri di obbligo. Non si creano mai criteri di obbligo direttamente con CA User Activity Reporting Module.

Criteri di accesso

Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	Concessione esplicita	ug:Administrator ug:Analyst ug:Auditor Win-Admin	read write	ApplicationInstance Policy User GlobalUser
d70238aa-caelm634ad71aa7-949d3bf0-a **etichette:** DataPolicy	SafeObligation	Concessione esplicita	Win-Admin	FulfillOnGrant	dataaccess/CALM/Data
Win-Admin System Access **etichette:** Win-Admin	SafeObject	Concessione esplicita Pre-distribuzione	Win-Admin	read	AppObject

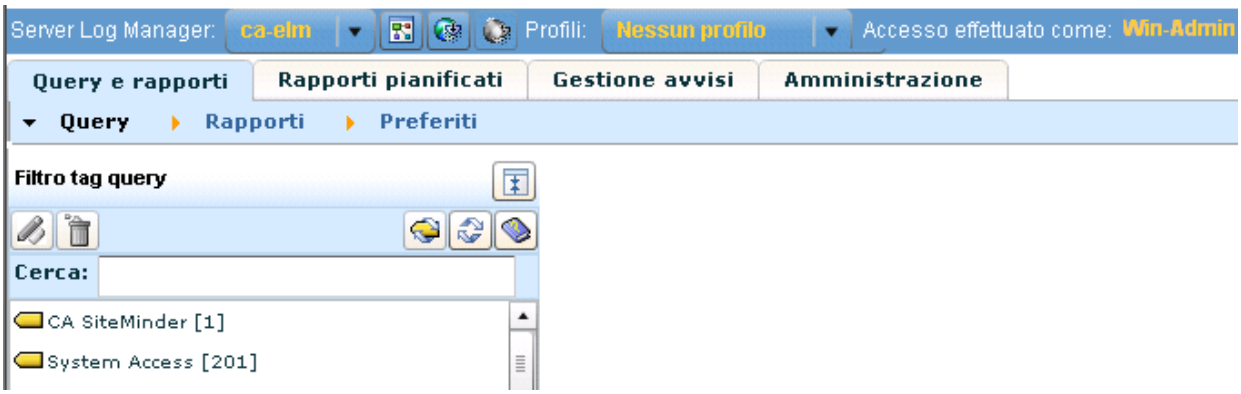
Ulteriori informazioni:

Creazione di un filtro di accesso (a pagina 103)

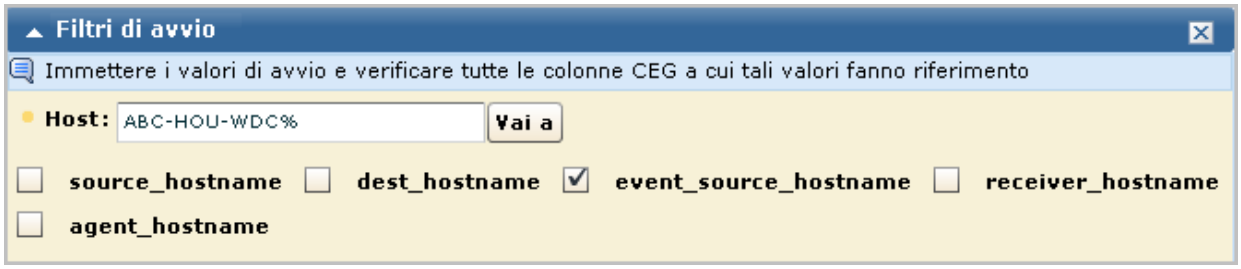
Passaggio 5: accesso come utente Win-Admin

Prima di creare criteri per un dato utente o gruppo utenti applicazione, accedere come tale utente o membro del gruppo e stabilire le operazioni consentite. Innanzitutto, verificare che le restrizioni previste siano attive. Dopodiché, verificare di essere in grado di eseguire le attività previste per tali utenti.

Per questo scenario, si prevede di essere in grado di visualizzare soltanto i rapporti o gli avvisi con il tag Accesso al sistema. In questo caso, l'unico filtro tag query disponibile è Accesso al sistema. Si verifica quindi quanto previsto.



Un modo rapido per eseguire il test di un filtro di accesso consiste nell'utilizzare la funzione Prompt. Tuttavia, questa funzione non è disponibile per l'utente Win-Admin. Tutte le query dei prompt presentano il tag "Visualizzatore eventi". L'accesso ai filtri prompt può essere garantito grazie al filtro del criterio calmTag=Visualizzatore eventi.



Il metodo più efficace per eseguire un test del filtro di accesso consiste nel verificare i dati visualizzati in un rapporto. Prendere in considerazione il seguente filtro di accesso. La colonna CEG event_logname inizia con NT- e la colonna di CEG event_source_hostname con ABC-MIL-WDC, un'abbreviazione della società ABC, città Milano, controller di dominio di Windows (WDC, Windows Domain Controller).

```
event_logname Like NT-% AND event_source_hostname Like ABC-HOU-WDC%
```

L'esempio seguente mostra un rapporto visualizzato dall'utente cui si applica questo filtro di accesso. Notare che i dati nella colonna Nome registro iniziano con NT- e che quelli nella colonna Origine iniziano con ABC-HOU-WDC.

System Access - All Events

Gravità	Date	Source	Utente	Azione	Nome registro	Classe
Informazioni	Giovedì 15/10/2009 16:19:	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informazioni	Giovedì 15/10/2009 16:19:	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informazioni	Giovedì 15/10/2009 16:19:	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informazioni	Giovedì 15/10/2009 16:19:	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informazioni	Giovedì 15/10/2009 16:19:	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informazioni	Giovedì 15/10/2009 16:19:	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informazioni	Giovedì 15/10/2009 16:19:	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informazioni	Giovedì 15/10/2009 16:19:	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informazioni	Giovedì 15/10/2009 16:19:	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informazioni	Giovedì 15/10/2009 16:19:	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informazioni	Giovedì 15/10/2009 16:19:	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informazioni	Giovedì 15/10/2009 16:19:	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informazioni	Giovedì 15/10/2009 16:19:	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informazioni	Giovedì 15/10/2009 16:19:	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informazioni	Giovedì 15/10/2009 16:19:	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informazioni	Giovedì 15/10/2009 16:19:	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informazioni	Giovedì 15/10/2009 16:19:	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informazioni	Giovedì 15/10/2009 16:19:	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management
Informazioni	Giovedì 15/10/2009 16:19:	ABC-HOU-WDC05	user01	Account Creation	NT-Security	Account Management

Passaggio 6: estensione delle azioni garantite

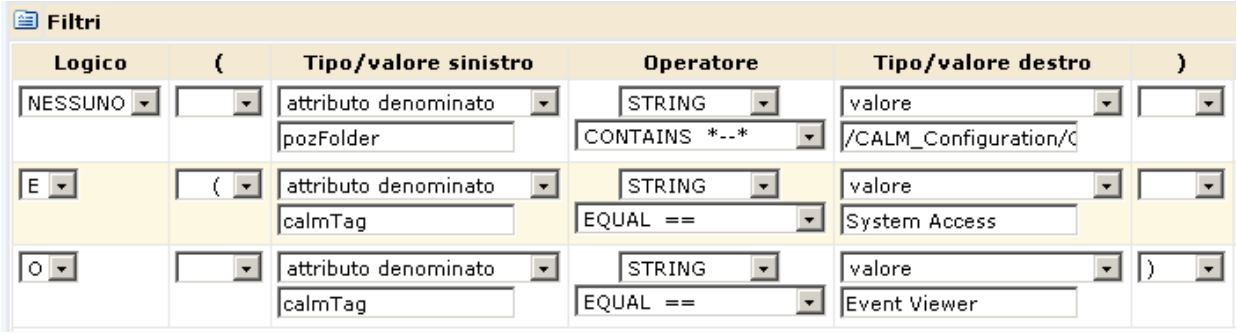
I criteri e i filtri di accesso definiti nei passaggi 2, 3 e 4 di questo esempio consentono all'utente Win-Admin di visualizzare i rapporti di accesso al sistema, con limitazioni sui dati. Se dispone solo di questo tipo di accesso, l'utente Win-Admin non può pianificare un rapporto, un avviso o annotare un rapporto. Per fare queste cose, aggiungere Win-Admin al criterio di accesso al server di rapporto per analisti e revisori e al criterio di creazione-pianificazione-annotazione per analisti. Seguono esempi di questi criteri a cui viene aggiunto l'utente Win-Admin:

Analyst Auditor Report Server Access Policy Analyst ,Auditor can Schedule Reports and Alerts against all available Report Servers	SafeObject	Concessione esplicita	ug:Analyst ug:Auditor	read	AppObject
Analyst Create-Schedule-Annotate policy Analyst can create/schedule Reports, create profiles, schedule Action Alerts,Annotate Reports	CALM	Concessione esplicita	ug:Analyst	create schedule annotate	Report Alert Tag

Perché Win-Admin possa creare un rapporto, occorre che l'accesso in scrittura venga aggiunto al criterio di accesso al sistema Win-Admin. Per fare ciò, aprire il criterio di accesso al sistema Win-Admin per modificarlo e aggiungere la scrittura alle azioni consentite.

Win-Admin System Access Win-Admin Report View POI	SafeObject	Concessione esplicita	Win-Admin	read	AppObject

Perché Win-Admin possa usare i prompt, il filtro per l'accesso al sistema Win-Admin può essere modificato in modo da rendere l'attributo calmTag equivalente ad Accesso al sistema o a Visualizzatore eventi.



Filtri

Logico	(	Tipo/valore sinistro	Operatore	Tipo/valore destro	)
NESSUNO		attributo denominato pozFolder	STRING CONTAINS *--*	valore /CALM_Configuration/C	
E	(	attributo denominato calmTag	STRING EQUAL ==	valore System Access	
O		attributo denominato calmTag	STRING EQUAL ==	valore Event Viewer	)

Limitazione dell'accesso a un ruolo: scenario per analisti PCI

È possibile creare un ruolo simile a un ruolo predefinito e realizzare rapidamente criteri modellati sui criteri predefiniti. Il ruolo definito dall'utente può essere simile al ruolo predefinito perché fornisce lo stesso accesso agli stessi tipi di risorsa, ma è diverso perché limita l'accesso basato su un filtro non presente nel ruolo predefinito. Possono esistere diversi criteri ai quali questo ruolo predefinito è stato aggiunto come identità. Se la configurazione di un criterio qualsiasi è tale da applicarsi al nuovo ruolo, occorre soltanto aggiungere il nuovo ruolo al criterio esistente. Se la configurazione è tale che occorre modificare tipo, risorse, azioni o filtri, è possibile creare un nuovo criterio dalla copia di uno esistente.

Questo esempio aiuta a creare un ruolo per un analista che utilizza soltanto rapporti dotati di tag PCI. Il criterio associato a questo ruolo viene creato dalla copia di un criterio esistente per tutti gli analisti.

Il processo prevede le seguenti procedure:

1. Pianificare i criteri necessari. Iniziare a identificare i criteri esistenti per supportare la creazione del nuovo ruolo.
2. Creare il nuovo gruppo utente dell'applicazione (ruolo), Analista PCI.
3. Concedere all'analista PCI un accesso di base a CA User Activity Reporting Module. Aggiungere questa identità al criterio di accesso all'applicazione CALM.

4. Conferire all'analista PCI lo stesso accesso ai server di rapporto degli analisti e creare le medesime abilità di rapporto. Aggiungere l'identità Analista PCI ai criteri identificati.
5. Limitare l'acceso ai rapporti che dispongono del calmTag PCI. Utilizzare il criterio che garantisce la capacità di visualizzare e modificare i rapporti come un modello da modificare.
6. Assegnare il ruolo di analista PCI a un utente di prova per la valutazione.
7. Accedere come utente di prova e valutare l'accesso.

   Se l'accesso consentito dal ruolo e dai criteri funziona come previsto, assegnare il ruolo a tutte le persone incaricate di analizzare i rapporti PCI.

Passaggio 1: pianificazione del ruolo e dei criteri da creare

Si supponga di voler creare un ruolo simile a quello dell'analista, ma di limitarne l'accesso ai rapporti e alle query relative al PCI. Scegliere un nome per il ruolo che ne descriva la funzione, ad esempio: Analista PCI.

Prima di iniziare a creare nuovi ruoli (o gruppi utente dell'applicazione), tenere presenti i criteri necessari a supportarli. Si consiglia di identificare i criteri esistenti che possono essere utilizzati come modelli. In Identità, cercare il ruolo simile a quello che si sta creando.

In questo caso, il ruolo è ug:Analista. In Criteri di ricerca, selezionare Mostra criteri corrispondenti all'identità, inserire l'identità **ug:Analista** e fare clic su Vai a. I criteri visualizzati includono quelli per Tutte le identità e quelli in cui ug:Analista viene nominato esplicitamente in Identità.

Criteri di accesso

<< < 1 / 1 > >>

Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	Concessione esplicita	ug:Administrator ug:Analyst ug:Auditor Win-Admin	read write	ApplicationInstance AppObject Policy User GlobalUser
Analyst Auditor Report Server Access Policy Analyst ,Auditor can Schedule Reports and Alerts against all available Report Servers	SafeObject	Concessione esplicita	ug:Analyst ug:Auditor	read	AppObject
Analyst Create-Schedule-Annotate policy Analyst can create/schedule Reports, create profiles, schedule Action Alerts,Annotate Reports	CALM	Concessione esplicita	ug:Analyst	create schedule annotate	Report Alert Tag Profile
Analyst Report View-Edit Policy Analyst can View/Edit any Report	SafeObject	Concessione esplicita	ug:Analyst	read write	AppObject

Di seguito sono elencati i nomi dei criteri che includono questo ruolo:

- In Scoping, Accesso all'applicazione CALM
- In Scoping, Criterio di accesso al server di rapporto per analisti e revisori
- In Scoping, Criterio di visualizzazione-modifica rapporti per analisti
- In CALM, Criterio di creazione-pianificazione-annotazione per analisti

Esaminare la definizione di ognuno dei criteri candidati e determinare quale delle azioni seguenti intraprendere:

- Aggiungere il nuovo ruolo come identità cui si applica questo criterio. È la scelta migliore se il criterio viene applicato al nuovo ruolo senza modifiche.

  In questo caso, tale azione è appropriata per i criteri seguenti:

  - Accesso all'applicazione CALM, che definisce tutte le identità che possono accedere a CA User Activity Reporting Module.
  - Criterio di accesso al server di rapporto per analisti e revisori, che definisce tutte le identità che possono pianificare rapporti e avvisi a fronte di tutti i server di rapporto disponibili. Questo ruolo non richiede limitazioni per i server di rapporto.
  - Criterio di creazione-pianificazione-annotazione per analisti.
- Salvare il criterio con un nome nuovo e modificarne la definizione.

  In questo esempio, tale azione è appropriata per il criterio seguente, in cui la nuova copia include soltanto la nuova identità e dispone di un filtro aggiuntivo per limitare l'accesso in lettura/scrittura ai rapporti con il tag PCI:

  - Criterio di visualizzazione-modifica rapporti per analisti.

Passaggio 2: creazione del ruolo Analista PCI

È possibile creare un ruolo personalizzato che rappresenti tutte le attività che più utenti eseguono con l'applicazione CA User Activity Reporting Module. Il ruolo corrisponde al gruppo utente dell'applicazione.

Il primo passaggio per la limitazione di accesso per un ruolo prevede la creazione del ruolo.

Quando si crea un ruolo personalizzato che non è soprainsieme di un ruolo esistente, non eseguire una selezione dai gruppi utente disponibili.

Ulteriori informazioni:

Creazione di un gruppo utente delle applicazioni (ruolo) (a pagina 87)

Passaggio 3: aggiunta dell'analista PCI al criterio di accesso all'applicazione CALM.

Dopo la creazione di qualsiasi ruolo nuovo, il passaggio successivo prevede di assegnare a tale ruolo la capacità di accesso di base all'applicazione CA User Activity Reporting Module. Per impostazione predefinita, infatti, soltanto i ruoli predefiniti hanno accesso. Aggiungere questo gruppo applicazione al criterio di accesso per l'applicazione CALM.

Ulteriori informazioni:

Come garantire l'accesso ruolo personalizzato a CA User Activity Reporting Module (a pagina 88)

Passaggio 4: aggiunta dell'analista PCI ai criteri esistenti

Una volta identificati i criteri che valgono per un gruppo utente dell'applicazione di cui il nuovo ruolo è un sottoinsieme, aggiungere il nuovo ruolo all'elenco corrente delle identità.

In questo esempio, aggiungere il ruolo analista PCI ai seguenti criteri esistenti:

- Criterio di accesso al server di rapporto per analisti e revisori.
- Criterio di creazione-pianificazione-annotazione per analisti.

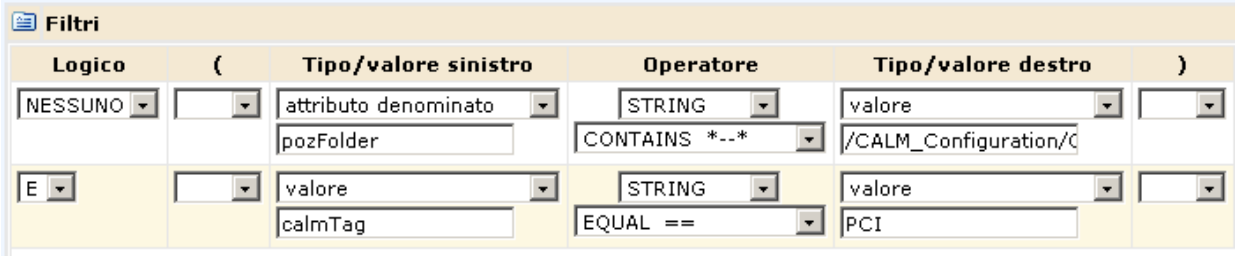
Ulteriori informazioni:

Aggiunta di un'identità a un criterio esistente (a pagina 90)

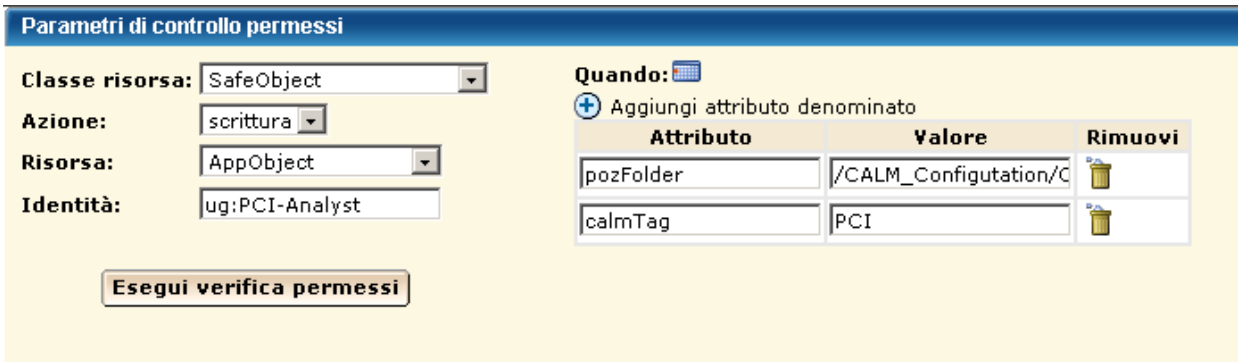
Passaggio 5: creazione di un criterio basato sul criterio di visualizzazione-modifica rapporti per analisti

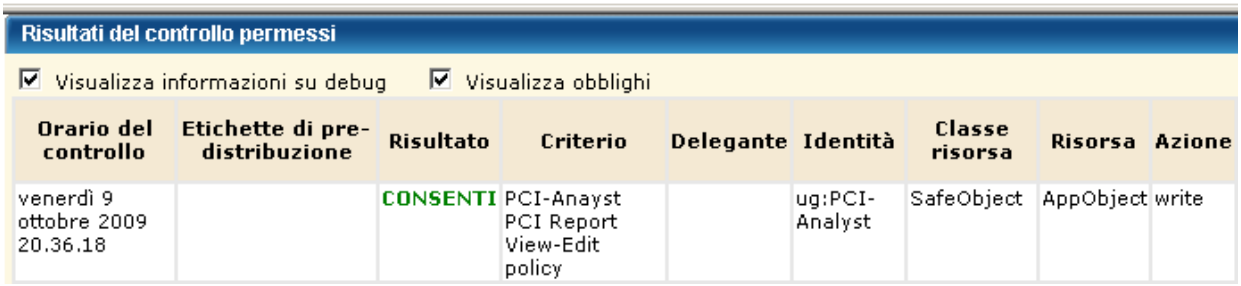
Quando si crea un criterio basato su un criterio esistente, si copia il criterio esistente e lo si salva con un nuovo nome. Successivamente, il criterio viene rinominato, si modifica la sua descrizione perché si adatti al nuovo ruolo e si sostituiscono le identità esistenti con quella nuova. Quando il criterio che si sta utilizzando come modello fornisce un accesso troppo ampio per il nuovo ruolo, occorre creare filtri che limitino tale accesso.

Nel caso dell'analista PCI, copiare il criterio di visualizzazione-modifica rapporti per analisti, salvarlo con un nuovo nome, aprire il nuovo criterio, sostituire l'identità con il gruppo analista PCI e aggiungere un filtro per limitare l'accesso ai rapporti con il calmTag PCI.



Si consiglia di testare un criterio basato su un criterio esistente proprio come si farebbe con uno completamente nuovo. Quando si verifica un criterio con un filtro, assicurarsi di inserire il filtro esattamente come appare nel criterio. Quando si specifica un nome gruppo per un'identità, assicurarsi di farlo precedere dal prefisso ug:, ad esempio ug:AnalistaPCI.





Ulteriori informazioni:

Creazione di un criterio basato su un criterio esistente (a pagina 98)
Verifica di un nuovo criterio (a pagina 100)

Passaggio 6: assegnazione del ruolo di analista PCI a un utente

Dopo aver creato un nuovo ruolo e i criteri a supporto, si consiglia di accedere come utente con questo ruolo per valutare se l'accesso fornito corrisponde alle proprie esigenze. Una volta verificato, il nuovo ruolo può essere aggiunto agli account di tutti gli utenti che devono eseguire le attività per le quali è stato progettato.

È possibile creare un account utente temporaneo allo scopo di verificare il nuovo ruolo e poi eliminare tale account una volta completato il test. Altrimenti, creare un utente chiamato Utente di prova e sostituire l'assegnazione del ruolo a ogni riutilizzo.

Ulteriori informazioni:

Assegnazione di un ruolo a un utente globale (a pagina 40)

Passaggio 7: accesso come analista PCI e valutazione dell'accesso

Verificare che i criteri siano sufficienti a limitare l'accesso a rapporti e avvisi dotati del tag PCI. Assegnare il ruolo di analista PCI a un utente e accedere a CA User Activity Reporting Module come quell'utente.

Visualizzare i tag di rapporto. Verificare che i rapporti visualizzabili siano solo quelli dotati del tag PCI.

Pianificare un rapporto. Verificare che i rapporti pianificabili siano solo quelli dotati del tag PCI.

Creare un rapporto. Verificare che l'unico tag disponibile per il nuovo rapporto sia il tag PCI.

Criteri di esempio per le integrazioni personalizzate

È possibile concedere a chi non ha il ruolo di amministratore la possibilità di creare integrazioni personalizzate tramite la realizzazione di un ruolo personalizzato, di un criterio CALM e di un criterio di scoping. Si può fornire ad altri utenti non amministratori la capacità di visualizzare le integrazioni personalizzate tramite la creazione di un ruolo personalizzato aggiuntivo con un criterio di scoping associato. Si aggiungono entrambi i criteri personalizzati al Criterio di accesso all'applicazione CALM e si assegnano gli utenti a questi ruoli.

La seguente procedura di esempio mostra come fare:

1. Creare un gruppo utente dell'applicazione di nome Crea-file-DM-XMP.
2. Creare un gruppo utente dell'applicazione di nome Visualizza-file-DM-XMP.
3. Garantire a Crea-file-DM-XMP e a Visualizza-file-DM-XMP l'accesso al prodotto CA User Activity Reporting Module.

Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	Concessione esplicita	ug:Administrator ug:Analyst ug:Auditor ug:Create-DM-XMP-Files ug:View-DM-XMP-Files	read write	ApplicationInstance AppObject Policy User GlobalUser

4. Creare un criterio CALM che garantisca a Crea-file-DM-XMP la capacità di creare file di mapping di dati e file di analisi del messaggio tramite CEG mentre è collegato a CA User Activity Reporting Module.

Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
Integration-Create policy Can create data mapping and message parsing files using common event grammar.	CALM	Concessione esplicita	Create-DM-XMP-Files	create	Integration

5. Creare un criterio di scoping che garantisca a Crea-file-DM-XMP la capacità di modificare e visualizzare i file DM e XMP personalizzati e salvati nella cartella EEM /CALM_Configuration/Content/Mapping o /CALM_Configuration/Content/Parsing tramite CEG.

Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
Edit-DM-XMP-Files with CEG Policy Can edit data mapping files and message parsing files using common event grammar saved to the EEM folders /CALM_Configuration/Content/...	SafeObject	Concessione esplicita	Create-DM-XMP-Files	read write	AppObject

Filtri	
DOVE	name:pozFolder *--* val:/CALM_Configuration/Content/Mapping
O	name:pozFolder *--* val:/CALM_Configuration/Content/Parsing

6. Creare un criterio di scoping che garantisca a Visualizza-file-DM-XMP la capacità di visualizzare i file DM e XMP personalizzati e salvati nella cartella EEM /CALM_Configuration/Content/Mapping o /CALM_Configuration/Content/Parsing.

   Nota: il criterio CEG garantisce a tutte le identità i diritti per visualizzare la CEG.

Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
View-DM-XMP-Files Can View data mapping files and message parsing files.	SafeObject	Concessione esplicita	View-DM-XMP-Files	read	AppObject

Filtri
DOVE (name:pozFolder *--* val:/CALM_Configuration/Content/Mapping O name:pozFolder *--* val:/CALM_Configuration/Content/Parsing)

7. Testare i criteri.
8. Assegnare utenti sia a Crea-file-DM-XMP che a Visualizza-file-DM-XMP.

Criteri di esempio per le regole di soppressione e riepilogo

È possibile fornire a chi non è amministratore la capacità di creare regole di soppressione e di riepilogo personalizzate tramite la creazione di un ruolo personalizzato, un criterio CALM e un criterio di scoping. Si può fornire ad altri utenti non amministratori la capacità di visualizzare le regole di soppressione e riepilogo personalizzate tramite la creazione di un ruolo personalizzato aggiuntivo con un criterio di scoping associato. Aggiungere entrambi i criteri personalizzati al criterio di accesso all'applicazione CALM e assegnare gli utenti a questi ruoli.

La seguente procedura di esempio mostra come fare.

1. Creare un gruppo utente dell'applicazione di nome Crea-regole-SOP-RIEP.
2. Creare un gruppo utente dell'applicazione di nome Visualizza-regole-SOP-RIEP.
3. Garantire a entrambi i ruoli l'accesso al prodotto CA User Activity Reporting Module.

Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
CALM Application Access This policy defines who all can access the CALM Application	SafeObject	Concessione esplicita	ug:Administrator ug:Analyst ug:Auditor ug:Create-Sup-Sum-Rules ug:View-Sup-Sum-Rules	read write	ApplicationInstance Policy User GlobalUser

4. Creare un criterio CA User Activity Reporting Module che garantisca agli utenti Crea-regole-SOP-RIEP la capacità di creare regole di soppressione o di riepilogo o di importarle mentre è collegato a CA User Activity Reporting Module.

Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
EventGrouping-Create policy Can create custom summarization and suppression rules or import rules.	CALM	Concessione esplicita	Create-Sup-Sum-Rules	create	EventGrouping

5. Creare un criterio di scoping che garantisca agli utenti Crea-regole-SOP-RIEP la capacità di visualizzare o modificare le regole di soppressione o riepilogo personalizzate salvate nella cartella EEM in /CALM_Configuration/Content/Rules/Suppression o /CALM_Configuration/Content/Rules/Summarization.

Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
View-Edit-SUP-SUM-Rules Can view or edit suppression and summarization rules that have been saved to Content/Rules/Summarization or Content/Rules Suppression folders.	SafeObject	Concessione esplicita	Create-Sup-Sum-Rules	read write	AppObject

Filtri			
DOVE	name:pozFolder	*--*	val:/CALM_Configuration/Content/Rules/Summarization
O	val:pozFolder	*--*	val:/CALM_Configuration/Content/Rules/Suppression

6. Creare un criterio di scoping che garantisca agli utenti Visualizza-regole-SOP-RIEP la capacità di visualizzare le regole di soppressione o di riepilogo personalizzate.

Nome/Descrizione	ResourceClassName	Opzioni	Identità	Azioni	Risorse
View-SUP-SUM-Rules Can view suppression and summarization rules that have been saved to Content/Rules/Summarization or Content/Rules Suppression folders.	SafeObject	Concessione esplicita	ug:View-Sup-Sum-Rules	read	AppObject

Filtri			
DOVE	name:pozFolder	*--*	val:/CALM_Configuration/Content/Rules/Summarization
O	val:pozFolder	*--*	val:/CALM_Configuration/Content/Rules/Suppression

7. Testare i criteri
8. Assegnare nuovi ruoli agli utenti. Ad esempio, può accadere che i revisori esterni vogliano visualizzare le regole di soppressione e riepilogo personalizzate. Per consentire questa operazione, è possibile assegnare loro un ruolo simile a Visualizza-regole-SOP-RIEP.

Un'alternativa alla creazione di due nuovi ruoli esplicitamente dedicati all'attività di creazione/modifica/visualizzazione e a quella di sola visualizzazione è l'espansione dei ruoli predefiniti di analista e revisore. Ad esempio è possibile eliminare i passaggi 1, 2, 3 e 8 della procedura seguente e assegnare invece l'analista come identità del criterio di creazione EventGrouping e Visualizza-regole-SOP-RIEP ed assegnare il gruppo utente revisore come identità di Visualizza-regole-SOP-RIEP.

Ulteriori informazioni:

Creazione di un gruppo utente delle applicazioni (ruolo) (a pagina 87)
Come garantire l'accesso ruolo personalizzato a CA User Activity Reporting Module (a pagina 88)
Verifica di un nuovo criterio (a pagina 100)
Assegnazione di un ruolo a un utente globale (a pagina 40)

Capitolo 5: Servizi e adapter CA

Questa sezione contiene i seguenti argomenti:

Attività servizi (a pagina 144)
Eliminazione di un host di servizio (a pagina 145)
Modificare le configurazioni globali (a pagina 145)
Modifica di una configurazione di servizio globale (a pagina 148)
Modifica di una configurazione di servizio locale (a pagina 149)
Configurazioni di servizio (a pagina 150)
Attività di configurazione degli adapter CA (a pagina 173)
Attività di Stato del sistema (a pagina 180)

Attività servizi

È possibile impostare configurazioni globali che vengono applicate a tutti i server CA User Activity Reporting Module. È possibile visualizzare e modificare due tipi di configurazioni di servizio individuali: una configurazione di servizio globale viene applicata a tutte le istanze di un singolo servizio nel proprio ambiente e una configurazione di servizio locale solo a un singolo host di servizi selezionato.

Nota: le configurazioni globali sono diverse dalle configurazioni di *servizi* globali: le prime controllano il comportamento di tutti i server CA User Activity Reporting Module e le seconde quello di un determinato servizio. Ad esempio, è possibile impostare l'intervallo di aggiornamento di tutti i servizi (configurazione globale) o i criteri di conservazione dei rapporti per tutti i server di rapporto (configurazione servizi globale).

È inoltre possibile visualizzare gli eventi di automonitoraggio dalle aree di configurazione dei servizi.

I servizi disponibili includono:

- Gestione agente
- Servizio di avviso
- Servizio di correlazione
- Deposito eventi di log
- Servizio incidenti
- Server ODBC
- Esegui query sul servizio
- Server rapporti
- Servizio test della regola
- Servizio di sottoscrizione
- Stato sistema

È possibile visualizzare i servizi in base al nome o all'host. È possibile utilizzare il servizio Stato del sistema per raccogliere le informazioni e controllare un server CA User Activity Reporting Module individuale.

Ulteriori informazioni:

Modifica di una configurazione di servizio globale (a pagina 148)
Modifica di una configurazione di servizio locale (a pagina 149)

Eliminazione di un host di servizio

Se viene disinstallato un server CA User Activity Reporting Module, è necessario eliminare la configurazione dell'host dal repository del server di gestione. La rimozione di questo riferimento manterrà il server aggiornato con l'elenco dei server CA User Activity Reporting Module registrati.

Per eliminare un host di servizio

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.

   Viene visualizzato l'Elenco servizi.

2. Fare clic su Host nella finestra di dialogo Mostra servizi per (si trova nella parte superiore dell'elenco).

   Viene visualizzato un elenco ad albero degli host di servizio.

3. Selezionare l'host da eliminare e fare clic su Elimina.

   L'host viene rimosso dall'elenco.

Importante: quando si elimina un host non appare alcun avviso. Facendo clic su Elimina, l'host viene rimosso immediatamente; pertanto, essere sicuri prima di procedere.

Modificare le configurazioni globali

È possibile impostare le configurazioni globali per tutti i servizi. Se si tenta di salvare valori non inclusi nell'intervallo consentito, per impostazione predefinita verrà utilizzato il valore massimo o minimo, a seconda dei casi. Molte delle impostazioni sono interdipendenti.

Per modificare le impostazioni globali

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.

   Viene visualizzato l'Elenco servizi.

2. Fare clic su Configurazione globale nell'Elenco servizi.

   Verrà visualizzato il riquadro dei dettagli Configurazione di servizio globale.

3. Modificare una delle seguenti impostazioni di configurazione:

Intervallo di aggiornamento

Indica la frequenza, in secondi, con cui i componenti del server applicheranno gli aggiornamenti di configurazione.

Minimo: 30

Massimo: 86400

Timeout di sessione

Specifica la lunghezza massima di una sessione inattiva. Se viene abilitata la funzione di aggiornamento automatico, la sessione non scade mai.

Minimo: 10

Massimo: 600

Consenti aggiornamento automatico

Consente agli utenti di aggiornare automaticamente i report o le query. Questa impostazione consente agli amministratori di disabilitare globalmente l'aggiornamento automatico.

Frequenza di aggiornamento automatico

Specifica, in minuti, l'intervallo di tempo tra gli aggiornamenti della visualizzazione del rapporto. Questa impostazione dipende dalla selezione di Consenti aggiornamento automatico.

Minimo: 1

Massimo: 60

Abilita aggiornamento automatico

Imposta l'aggiornamento automatico in tutte le sessioni. Per impostazione predefinita, l'aggiornamento automatico non è abilitato.

Per visualizzare gli avvisi è necessario effettuare l'autenticazione

Impedisce ai revisori o ai prodotti di terze parti di visualizzare i feed RSS di avviso. Questa funzione è attivata per impostazione predefinita.

Rapporto predefinito

Consente di specificare il rapporto predefinito.

Abilita avvio del rapporto predefinito

Visualizza il rapporto predefinito facendo clic sulla sottoscheda Rapporti. Questa funzione è attivata per impostazione predefinita.

4. Modificare una delle seguenti impostazioni relative a rapporti e tag delle query:

   Nascondi tag di rapporto

   Impedisce la visualizzazione dei tag specificati negli elenchi di tag. Nascondendo i tag di rapporto, sarà più semplice visualizzare i rapporti disponibili.

   Nascondi tag delle query

   Consente di nascondere i tag selezionati. I tag nascosti non verranno visualizzati nell'elenco principale delle query o nell'elenco delle query di pianificazione degli avvisi. Nascondendo i tag di query, sarà possibile personalizzare la visualizzazione delle query disponibili.

5. Modificare una delle seguenti impostazioni dashboard:

   Abilita avvio dashboard predefinito

   Visualizza il dashboard predefinito facendo clic sulla scheda Query e rapporti. Questa funzione è attivata per impostazione predefinita.

   Dashboard predefinito

6. Modificare una delle seguenti impostazioni di profilo:

   Attivazione profilo predefinito

   Consente di impostare il profilo predefinito.

   Profilo predefinito

   Indica il profilo predefinito.

   Nascondi profili

   Consente di nascondere i profili selezionati. I profili nascosti non verranno visualizzati quando si aggiorna l'interfaccia o quando scade l'intervallo di aggiornamento. Nascondendo i profili, sarà possibile personalizzare la visualizzazione dei profili disponibili.

   Nota: fare clic su Reimposta per ripristinare i valori dell'ultimo salvataggio. Sarà possibile ripristinare una o più modifiche, finché non le si salva. Una volta salvate le modifiche, sarà necessario reimpostarle singolarmente.

7. Fare clic su Salva.

Modifica di una configurazione di servizio globale

È possibile modificare le configurazioni di servizio globali. Si tratta di impostazioni che si applicano a tutte le istanze di un dato servizio nel proprio ambiente. Una configurazione di servizio globale *non* sostituisce le impostazioni di servizio locali che differiscono dalle impostazioni globali.

I valori massimi e minimi di configurazione sono esaminati in dettaglio nelle sezioni specifiche del servizio. Se si tenta di salvare i valori al di fuori dell'intervallo concesso, CA User Activity Reporting Module ripristina per impostazione predefinita i valori minimi o massimi appropriati.

Per modificare una configurazione di servizio globale

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.

   Viene visualizzato l'Elenco servizi.

2. Selezionare il servizio di cui si vuole modificare la configurazione.

   Nel riquadro dei dettagli viene visualizzata la configurazione di servizio globale.

3. Apportare le modifiche desiderate alla configurazione.

   Nota: è possibile fare clic su Reimposta per ripristinare l'ultimo valore salvato nei campi di immissione. È possibile reimpostare una o più modifiche fino a quando si fa clic su Salva. Una volta salvate le modifiche, sarà necessario ripristinarle individualmente.

4. Una volta terminate tutte le modifiche, fare clic su Salva.

   Tutti i cambiamenti apportati alla configurazione vengono applicati a tutti gli host del servizio selezionato, a meno che abbiano diverse impostazioni locali.

Modifica di una configurazione di servizio locale

È possibile visualizzare o modificare le configurazioni di servizio locali in base al servizio o al server host. Le configurazioni di servizio locali consentono di controllare i servizi o le impostazioni che potrebbero non essere adatte o richieste per l'intero ambiente, ignorando le impostazioni globali dei soli host specificati. Ad esempio, si supponga di voler impostare un server CA User Activity Reporting Module specifico per memorizzare gli avvisi più a lungo degli altri. È possibile controllare questa opzione con una configurazione locale.

I valori massimi e minimi di configurazione sono esaminati in dettaglio nelle sezioni specifiche del servizio. Se si tenta di salvare i valori al di fuori dell'intervallo concesso, CA User Activity Reporting Module ripristina per impostazione predefinita i valori minimi o massimi appropriati.

Per modificare una configurazione di servizio locale

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.

   Viene visualizzato l'Elenco servizi.

2. Fare clic sulla freccia accanto al servizio del quale si vuole modificare la configurazione.

   La visualizzazione del servizio si espande per mostrare i singoli host di servizio.

3. Fare clic sull'host di servizio desiderato.

   Nel riquadro dei dettagli viene visualizzata la configurazione del servizio.

4. Apportare le modifiche desiderate alla configurazione. In ogni campo di immissione, menu o controllo della configurazione locale viene visualizzato un pulsante di configurazione locale/globale, che permette di passare da uno stato all'altro.

   Configurazione globale:

   Configurazione locale:

   Un clic sul pulsante permette di passare dall'impostazione globale a quella locale e rende il valore associato disponibile all'uso. Tale valore deve sempre essere impostato per la configurazione locale perché l'impostazione abbia effetto; se fosse impostato sulla configurazione globale, per quel listener sarebbe attiva l'impostazione globale.

Nota: facendo clic su Reimposta, è possibile visualizzare i valori di configurazione salvati più recenti per tutte le configurazioni disponibili. È possibile reimpostare una o più modifiche fino a quando si fa clic su Salva. Una volta salvate le modifiche, sarà necessario ripristinarle individualmente.

5. Una volta terminate tutte le modifiche, fare clic su Salva.

   Ogni modifica apportata viene applicata soltanto all'host di servizio selezionato.

Configurazioni di servizio

Questa sezione contiene dettagli e linee guida di servizio da tenere in considerazione per modificare la configurazione dei seguenti servizi CA User Activity Reporting Module:

- Servizio di avviso: controlla le impostazioni di recapito per gli avvisi, inclusi i server SMTP, CA IT PAM e le impostazioni dei trap SNMP.
- Servizio di correlazione: controlla le regole di correlazione e l'inoltro degli eventi per la creazione degli incidenti.
- Deposito eventi di log: archivia tutti gli eventi non elaborati perfezionati e registrati.
- Servizio incidenti: controlla la creazione e l'archiviazione di incidenti derivanti dalla correlazione di eventi.
- Server ODBC: consente di accedere al deposito eventi di log di CA User Activity Reporting Module da un'applicazione esterna, come BusinessObjects Crystal Reports.
- Server di rapporto: controlla la distribuzione, formattazione e memorizzazione di rapporti e avvisi.
- Servizio di sottoscrizione: inoltra gli aggiornamenti di contenuto e di configurazione al server di gestione e gli aggiornamenti binari ai client di sottoscrizione.

Ulteriori informazioni:

Sottoscrizione (a pagina 227)

Considerazioni sul servizio di avviso

Il servizio di avviso controlla il recapito di avvisi. Dall'area di configurazione del servizio di avviso è possibile eseguire le seguenti attività:

- Nell'area Impostazioni di posta elettronica, impostare il server di posta elettronica, l'indirizzo di posta elettronica dell'amministratore, la porta SMTP e le informazioni di autenticazione per il recapito degli avvisi.
- Configurare l'integrazione di CA IT PAM per gli avvisi.
- Configurare l'integrazione ObserveIT.
- Impostare i trap SNMP per il recapito degli avvisi.

Ulteriori informazioni:

Configurazione di CA User Activity Reporting Module per il funzionamento con ObserveIT. (a pagina 155)
Configurare l'integrazione con una destinazione di trap SNMP (a pagina 157)

Configurazione dell'integrazione CA IT PAM

È possibile configurare l'integrazione di CA IT PAM in modo da sfruttare uno o entrambi i seguenti tipi di processi di CA IT PAM.

- Processo di output di evento/alert: processo che richiama l'elaborazione su un sistema di terze parti
- Processo di valori dinamici: processo che accetta una chiave di input e ne restituisce i valori correnti sotto forma di file con valori delimitati da virgole (*.csv)

La seguente procedura è valida per entrambe le impostazioni.

Per configurare l'integrazione CA IT PAM

1. Fare clic sulla scheda Amministrazione, quindi selezionare sottoscheda Servizi.
2. Fare clic su Servizio di avviso.

   Viene visualizzata la finestra di dialogo della configurazione di servizio globale: Alerting Service (Servizio Avvisi).

3. Scorrere fino all'area CA IT PAM.
4. Inserire il nome di host completo del server su cui è installato CA IT PAM, accettare il numero di porta predefinito, ovvero 8080, ed inserire credenziali valide per l'accesso a CA IT PAM.
5. Eseguire le seguenti operazioni per il processo di output di evento/alert nella sezione Processo di output evento/alert:
   a. Se si importa il file EventAlertOutput.xml campione per utilizzarlo, accettare la voce predefinita per Processo di output evento/alert. In caso contrario, sostituire questa voce con il nome del processo di output di evento/alert personalizzato, preceduto dal relativo percorso.

      Nota: è possibile visualizzare il nome ed il percorso del processo in Cartelle nel client ITPAM.

   b. Se si importa il file EventAlertOutput.xml campione per utilizzarlo, definire come segue i valori predefiniti di ReportedBy, Severity, Priority ed EndUser:
      a. Selezionare un parametro e fare clic su Aggiungi valore predefinito.

         Verrà visualizzata la finestra di dialogo Aggiungi valore.

      b. Immettere il valore predefinito e fare clic su OK.
   c. Se si specifica un processo personalizzato di output di evento/alert, eliminare i parametri visualizzati ed aggiungere i paramerti personalizzati. A questo punto, definire il valore predefinito per ognuno di essi.

6. Nella sezione Aggiornamento elenco con chiave, eseguire l'aggiornamento pianificato dell'elenco con chiave, eseguire le operazioni riportate di seguito:
   a. Selezionare il server per l'aggiornamento dell'elenco con chiave dall'elenco dei server predefiniti.
   b. Selezionare l'opzione Abilitato.

      Vengono visualizzati i parametri richiesti per l'impostazione della pianificazione.
   c. Selezionare il fuso orario e l'ora di inizio per l'esecuzione dell'utilità di pianificazione dell'aggiornamento.
   d. Selezionare la frequenza di ripetizione dell'esecuzione dell'utilità di pianificazione dell'aggiornamento e specificare le informazioni richieste.
7. Fare clic su Salva.

   Viene visualizzato il messaggio di conferma: Modifiche configurazione salvate con successo. La configurazione IT PAM viene completata.

Ulteriori informazioni:

Creazione di un elenco con chiave (a pagina 353)

Integrazione ObserveIT

È possibile integrare CA User Activity Reporting Module con ObserveIT per analizzare le registrazioni delle sessioni utente.

ObserveIT consente di effettuare le seguenti operazioni:

- Monitoraggio delle attività di configurazione di tutti gli utenti
- Monitoraggio di tutte le attività utente sospette
- Generazione di rapporti per tutte le attività utente

È possibile utilizzare una o più istanze di ObserveIT.

Nota: per ulteriori informazioni sul monitoraggio delle attività utente, consultare la documentazione ObserveIT.

Ulteriori informazioni:

Considerazioni sull'integrazione (a pagina 154)
Configurazione di CA User Activity Reporting Module per il funzionamento con ObserveIT. (a pagina 155)
Visualizzazione della registrazione di una sessione utente (a pagina 156)

Integrazione di CA User Activity Reporting Module con ObserveIT

Questa sezione fornisce all'amministratore una descrizione della procedura per l'integrazione di CA User Activity Reporting Module con ObserveIT.

Per integrare CA User Activity Reporting Module con ObserveIT, eseguire le seguenti operazioni:

- Configurare CA User Activity Reporting Module per il funzionamento con ObserveIT.
- Visualizzare la registrazione di una sessione utente.

Considerazioni sull'integrazione

CA User Activity Reporting Module supporta l'integrazione con ObserveIT 5.2.5.1. Per integrare CA User Activity Reporting Module con ObserveIT, eseguire le operazioni riportate a continuazione:

- Verificare che il server ObserveIT sia stato installato.
- Se si desidera analizzare le registrazioni delle sessioni utente da più istanze di ObserveIT, verificare che il server di gestione centralizzata ObserveIT sia stato installato.
- Se si desidera raccogliere i log ObserveIT da un'origine di eventi, verificare di aver eseguito la distribuzione di un connettore ObserveIT su ciascun database ObserveIT dell'origine evento. Per ulteriori informazioni sul connettore ObserveIT, consultare la *Guida al connettore per ObserveIT*.

Nota: per informazioni sull'installazione di ObserveIT, consultare la documentazione di ObserveIT.

Configurazione di CA User Activity Reporting Module per il funzionamento con ObserveIT.

L'utilizzo di CA User Activity Reporting Module con ObserveIT consente di visualizzare la registrazione delle sessioni utente. Per eseguire l'integrazione di CA User Activity Reporting Module con ObserveIT, è necessario configurare il server ObserveIT dall'interfaccia CA User Activity Reporting Module.

Per configurare CA User Activity Reporting Module per il funzionamento con ObserveIT.

1. Fare clic su Amministrazione, Servizi, quindi selezionare Servizio di avviso.

   Viene visualizzata la finestra di dialogo Configurazione di servizio globale: Servizio di avviso. Per impostazione predefinita, viene visualizzata la scheda Amministrazione.

   Nota: è possibile configurare un server CA User Activity Reporting Module specifico per utilizzare ObserveIT a livello di configurazione locale.

2. Nel riquadro ObserveIT, completare i seguenti campi con i dati corrispondenti, quindi fare clic su Salva:

   URL server ObserveIT

   Specifica l'indirizzo del server ObserveIT.

   Nota: se si utilizza una singola istanza ObserveIT, è necessario specificare l'indirizzo del server ObserveIT nel seguente formato:

   `http://observeit_appserver:port_number_used_to_install_ObserveIT/ObserveIT`

   Se si utilizzano più istanze ObserveIT, è necessario specificare l'indirizzo del server di gestione centralizzata nel seguente formato:

   `http://observeit_centralizedmanagementserver/ObserveITCentralizedManagement/`

   Nome utente

   Specifica il nome utente dell'amministratore che dispone dei diritti di accesso al server ObserveIT.

   Password

   Specifica la password associata all'amministratore del server ObserveIT.

3. (Facoltativo) Fare clic su Verifica connessione.

   La connessione al server ObserveIT viene verificata. Se la connessione viene eseguita correttamente, viene visualizzato il messaggio: Informazioni di connessione al server ObserveIT convalidate con successo. Il server applicazioni ObserveIT viene configurato dal server CA User Activity Reporting Module.

Ulteriori informazioni:

Considerazioni sull'integrazione (a pagina 154)
Visualizzazione della registrazione di una sessione utente (a pagina 156)

Visualizzazione della registrazione di una sessione utente

CA User Activity Reporting Module consente di visualizzare una sessione utente registrata da ObserveIT. È necessario disporre dei diritti di amministratore o analista per visualizzare la registrazione di una sessione utente. È possibile visualizzare la registrazione di una sessione utente avviando il visualizzatore query attraverso l'API di CA User Activity Reporting Module.

Per visualizzare la registrazione di una sessione utente

1. Fare clic con il pulsante destro su un evento in un rapporto, quindi selezionare Analisi host per registrazione sessione utente.

   Viene visualizzata la finestra di dialogo Eventi di registrazione della sessione utente ObserveIT. La finestra di dialogo visualizza tutte le registrazioni delle sessioni utente disponibili per il periodo di tempo corrispondente all'evento selezionato e all'ora corrente.

2. Fare clic sull'icona video della sessione che si desidera visualizzare.

   Nota: l'icona video è abilitata solo se è presente un evento nel periodo di tempo selezionato.

   Viene visualizzata la finestra ObserveIT - Slide Viewer. La registrazione della sessione utente selezionata viene riprodotta.

Ulteriori informazioni:

Considerazioni sull'integrazione (a pagina 154)
Configurazione di CA User Activity Reporting Module per il funzionamento con ObserveIT. (a pagina 155)

Configurare l'integrazione con una destinazione di trap SNMP

Configurare l'integrazione SNMP come parte della configurazione globale di servizio per il server di rapporto. La configurazione corrisponde all'indirizzo IP e alla porta della destinazione dei trap SNMP.

È possibile configurare l'integrazione SNMP sia prima che dopo aver preparato il prodotto di destinazione a ricevere e ad interpretare i trap SNMP di CA User Activity Reporting Module.

Quando si crea un avviso indirizzato al destinatario di un trap SNMP, è possibile specificare una o più destinazioni. Questa configurazione sarà quella predefinita. L'impostazione predefinita verrà applicata a tutti server elencati in Server di rapporto.

Per configurare l'integrazione SNMP

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
2. Fare clic su Alerting Service (Servizio Avvisi)

   Viene visualizzata la finestra di dialogo della configurazione di servizio globale: Alerting Service (Servizio Avvisi).
3. Scorrere fino all'area Configurazione SNMP.
4. Immettere l'indirizzo IP o il nome host del server di destinazione per le trap SNMP.
5. Accettare la porta predefinita, 162, oppure modificarla.
6. Fare clic su Salva.

Considerazioni sul servizio di correlazione

Il servizio di correlazione controlla le regole applicate al server di correlazione. Quando si applica una regola, il servizio diventa attivo.

É possibile associare destinazioni di notifica alle regole, nonché attivare o disattivare le regole dalla pagina di configurazione del Servizio di correlazione. È possibile selezionare i server CA User Activity Reporting Module per il reindirizzamento degli eventi al server di correlazione specificato, oppure impostare un limite evento.

Limite evento

Definisce il numero di eventi conservati per incidente l'opzione di accumulo è abilitata. Il Limite evento consente di evitare il traffico eccessivo determinato dalla correlazione durante i periodi con un livello di attività elevato. Quando tale limite viene raggiunto, gli eventuali eventi aggiuntivi vengono persi. Ad esempio, se il limite è impostato su 100, una regola può accumulare fino a un massimo di 100 eventi registrati, inclusi l'evento o eventi di iniziali corrispondenti. L'accumulo eventi continua fino al raggiungimento del limite evento, o più generalmente, quando i valori di intervallo o di limite reimpostano la regola.

Inoltre, la deselezione delle regole di correlazione applicate consente di rimuovere tali regole.

Per rimuovere regole dall'elenco di regole applicate

1. Evidenziare la riga relativa alla regola di correlazione che si desidera rimuovere.
2. (Facoltativo) Per selezionare più righe, fare clic tenendo premuto il tasto CTRL oppure CTRL+MAIUSC.
3. Fare clic su Rimuovi.

   Le regole selezionate vengono rimosse dall'elenco attivo.
4. Fare clic su Salva per confermare la configurazione. Se non si è effettuato il salvataggio, è possibile fare clic su Reimposta per ripristinare le regole rimosse nell'elenco.

   Nota: questa procedura rimuove le regole di correlazione solo dall'elenco attivo e non dalla libreria delle regole.

Considerazioni sul deposito eventi di log

Il deposito eventi di log utilizza un sistema di archiviazione federato in cui ogni server host mantiene il proprio deposito eventi di log locale e la capacità di contattarne altri nel proprio ambiente. Quando si interroga un server per informazioni sull'evento, è possibile che avvii la ricerca nel proprio deposito eventi di log, così come in altri depositi connessi mediante la federazione. Questo accorgimento consente l'archiviazione e la memorizzazione flessibile dei dati degli eventi.

Le impostazioni relative al deposito eventi di log consentono di specificare la frequenza e la posizione di archiviazione dei dati. Vengono interrogati sia i depositi eventi di log hot (attivi) che le informazioni sugli eventi di log warm (archiviate). Le informazioni sugli eventi in archiviazione cold (remota) non vengono interrogate.

È possibile configurare le seguenti impostazioni di archiviazione e del deposito eventi di log:

Numero massimo di righe

Consente di impostare il numero massimo di eventi che il database hot del deposito eventi di log è in grado di contenere. Se il conteggio degli eventi raggiunge questo valore, il log eventi comprime tutte le informazioni sugli eventi nel database hot e le trasferisce al database warm.

Minimo: 50000

Massimo: 100000000

Giorni di archiviazione massimi

Imposta il numero di giorni durante i quali i file archiviati vengono memorizzati nell'archiviazione prima di essere eliminati.

Minimo: 1

Massimo: 28000

Spazio su disco di archiviazione

Definisce la percentuale di spazio rimanente su disco che attiva la cancellazione automatica dei file archiviati meno recenti. Ad esempio, il valore predefinito è 10. Quando lo spazio disponibile del deposito eventi di log scende al di sotto del 5 percento, il log eventi rimuove i file archiviati meno recenti per liberare spazio.

Minimo: 10

Massimo: 90

Criterio di esportazione

Definisce il numero di ore di conservazione di un file ripristinato sull'archivio (defrosted) nel deposito eventi di log prima di essere eliminato.

Minimo: 0

Massimo: 168

Regole di aggregazione/soppressione

Controlla quali sono le regole di aggregazione o soppressione applicate agli eventi ricevuti. Prima di avviare la ridefinizione degli eventi, è necessario che l'amministratore applichi le nuove regole di aggregazione o di soppressione.

Regole di inoltro

Determina quali regole disponibili di inoltro degli eventi vengono applicate agli eventi ricevuti.

Figlio della federazione

Controlla quali depositi eventi di log disponibili sono impostati come figli del server corrente. L'impostazione consente di impostare strutture di federazione separate e di controllare i livelli di accesso alle query. L'impostazione è disponibile soltanto come impostazione locale.

Le impostazioni di registrazione controllano il modo in cui i moduli CA User Activity Reporting Module registrano i messaggi interni. Sono disponibili soltanto come impostazioni locali. Solitamente le impostazioni di registrazione vengono utilizzate per la risoluzione dei problemi. Come regola generale non è necessario modificare tali impostazioni. Prima di eseguire l'operazione, è necessario disporre di una conoscenza approfondita dei file di log e del processo di registrazione.

Livello di log

Definisce il tipo e il livello di dettaglio presenti nel file in registrazione. L'elenco a discesa è disposto in ordine crescente di dettaglio.

Applica a tutti i registratori

Determina se l'impostazione del livello di log sostituisce tutte le impostazioni di log dal file delle proprietà del log. Questa impostazione si applica soltanto quando l'impostazione del livello di log è inferiore (ovvero più dettagliata) rispetto a quella predefinita.

Le impostazioni di archiviazione automatica consentono di abilitare e controllare i processi di archiviazione del database pianificati, i quali spostano i database warm a un server remoto.

Nota: prima di spostare i processi di database pianificati da un server CA User Activity Reporting Module all'altro, o a un server remoto, è necessario configurare l'autenticazione non interattiva tra i server. Per ulteriori informazioni, vedere la sezione relativa alla configurazione dell'autenticazione non interattiva della *Guida all'implementazione di CA User Activity Reporting Module*.

È possibile impostare i seguenti valori di archiviazione automatica:

Abilitato

Imposta l'attivazione di un processo di archiviazione automatica. L'archiviazione automatica sfrutta l'utilità SCP sulla base delle altre impostazioni.

Tipo backup

Controlla il tipo di backup: si tratta di un'archiviazione completa che copia tutte le informazioni del database, o un'archiviazione incrementale che copia tutti i database di cui non è ancora stato eseguito il backup.

Impostazione predefinita: incrementale

Frequenza

Specifica se il processo di archiviazione viene eseguito ogni giorno o ogni ora. Un processo giornaliero viene eseguito all'ora stabilita mediante l'orologio dell'ora di inizio. Un processo orario viene eseguito ad ogni ora della giornata.

Ora di inizio

Definisce l'ora di inizio di un processo di archiviazione giornaliero, in base all'ora locale del server. Il valore è un orologio di 24 ore.

Limiti: 0-23, dove 0 indica la mezzanotte e 23 le 11.00 di sera.

Utente EEM

Specifica l'utente che può eseguire una query di archiviazione, ricatalogare il database di archiviazione, avviare l'utilità LMArchive e lo script restore-ca-elm. È necessario che l'utente disponga di privilegi di amministratore.

Impostazione predefinita: utente amministratore Log Manager.

Password EEM

Specifica la password per l'utente i cui diritti sono definiti nel campo Utente EEM.

Server remoto

Specifica il nome host o l'indirizzo IP del server remoto sul quale il processo di archiviazione automatica copia le informazioni del database.

Utente remoto

Consente di specificare il nome utente utilizzato dall'utilità SCP per la connessione al server remoto.

Impostazione predefinita: caelmservice

Posizione remota

Specifica la destinazione del file di archiviazione sul server remoto.

Impostazione predefinita: /opt/CA/LogManager

Server ELM remoto

Indica se il server remoto è un server di gestione. In caso affermativo, il processo di archiviazione automatica elimina i database dal computer locale una volta completato il trasferimento. Viene quindi inviata una notifica al computer remoto per l'esecuzione di una ricatalogazione.

Intervallo di ricezione eventi di correlazione

Determina l'ampiezza della finestra temporale tollerata per la creazione degli incidenti. I valori Ora di fine variazione e Ora di inizio variazione consentono di impostare un valore successivo all'orario corrente del server CA User Activity Reporting Module (futuro) e precedente all'orario corrente del server CA User Activity Reporting Module (passato). Gli eventi al di fuori di tale finestra non verranno inoltrati per la correlazione.

Nota: i valori di ricezione degli eventi di correlazioni non vengono considerati per le regole di calcolo. Tali regole tengono in considerazione soltanto eventi con una durata inferiore a 5 minuti. Gli eventi con data e ora indicanti più di 5 minuti vengono ignorati, indipendentemente dal valore Ora di inizio variazione.

Ulteriori informazioni:

Archiviazione dei registri (a pagina 185)
Applicazione di una regola di soppressione o riepilogo (a pagina 533)

Considerazioni sul servizio incidenti

È possibile controllare il modo in cui il servizio incidenti archivia gli eventi e crea gli incidenti per un server CA User Activity Reporting Module selezionato. È possibile impostare i valori seguenti:

Data di scadenza

Specificare per quanti giorni il servizio conserva gli incidenti nel database incidenti. Se il valore è 0, gli eventi non vengono mai eliminati. Gli incidenti scaduti non vengono visualizzati.

Limite di generazione incidente

Specifica la frequenza con cui una singola regola di correlazione può creare incidenti, consentendo di ridurre gli incidenti multipli indesiderati. Per gli scopi dei limiti di generazione incidente, le diverse versioni di una stessa regola vengono considerate regole separate. Di conseguenza, se nell'ambiente sono state applicate più versioni di una regola, queste vengono limitate separatamente. I valori limite includono:

Abilitato

Indica se vengono applicati i limiti di generazione incidente.

Conteggio

Imposta un limite per il numero di incidenti generati da una singola regola. Questo valore opera in congiunzione con il valore Ora, se tale valore è superiore a 0. Quando vengono raggiunti questi valori, il Servizio incidenti applica il limite Durata del blocco. Se si imposta Conteggio su 3, e Ora su 10, il limite viene applicato quando una singola regola genera più di 3 eventi in 10 secondi.

Ora

Imposta una soglia, in secondi, per il numero di incidenti generati da una singola regola. Questo valore opera in congiunzione con il valore Conteggio, se tale valore è superiore a 0. Quando vengono raggiunti questi valori, il Servizio incidenti applica il limite Durata del blocco. Se si imposta Conteggio su 3, e Ora su 10, il limite viene applicato quando una singola regola genera più di 3 eventi in 10 secondi.

Durata del blocco

Specifica l'intervallo, in secondi, in cui la creazione di ulteriori incidenti da parte di una regola viene bloccata. Quando il limite viene raggiunto, la regola non crea incidenti finché non scade il tempo impostato.

Considerazioni su ODBC Server

È possibile installare un client ODBC o JDBC per accedere al deposito eventi di log di CA User Activity Reporting Module da un'applicazione esterna come SAP BusinessObjects Crystal Reports.

Da questa area di configurazione è possibile eseguire le seguenti attività:

- Abilitare o disabilitare l'accesso di ODBC e di JDBC al deposito eventi di log.
- Impostare la porta di servizio utilizzata per le comunicazioni fra il client ODBC o JDBC ed il server CA User Activity Reporting Module
- Specificare se le comunicazioni fra il client ODBC o JDBC e CA User Activity Reporting Module sono crittografate.

Le descrizioni dei campi sono le seguenti:

Abilita servizio

Indica se i client ODBC o JDBC possono accedere ai dati nel deposito eventi di log. Selezionare questa casella di controllo per abilitare l'accesso esterno agli eventi. Deselezionare la casella di controllo per disabilitare l'accesso esterno.

Il servizio ODBC non è attualmente compatibile con FIPS. Deselezionare questa casella di controllo per prevenire l'accesso di ODBC e JDBC in caso di esecuzione in modalità FIPS. In questo modo viene evitato l'accesso non conforme ai dati evento. Se si desidera disabilitare i servizi ODBC e JDBC per eseguire operazioni in modalità FIPS, assicurarsi di impostare questo valore per *ogni* server di una federazione.

Porta di ascolto del server

Specifica il numero di porta utilizzato dai servizi ODBC o JDBC. Il valore predefinito è 17002. Il server CA User Activity Reporting Module rifiuta i tentativi di connessione quando è specificato un valore diverso nella stringa di origine dati di Windows o dell'URL JDBC.

Crittografato (SSL)

Indica se utilizzare la crittografia per le comunicazioni fra il client ODBC ed il server CA User Activity Reporting Module. Il server CA User Activity Reporting Module rifiuta i tentativi di connessione quando il valore in origine dati di Windows o nell'URL JDBC non corrisponde a questa impostazione.

Timeout di sessione (minuti)

Specifica il numero di minuti in cui una sessione inattiva resterà aperta prima che si chiuda automaticamente.

Livello di log

Definisce il tipo e il livello di dettaglio presenti nel file in registrazione. L'elenco a discesa è disposto in ordine di dettaglio: la prima voce corrisponde alla meno dettagliata.

Applica a tutti i registratori

Controlla se l'impostazione del livello di log sovrascrive tutte le impostazioni di log dal file delle proprietà del log. Questa impostazione si applica soltanto quando l'impostazione del livello di log è inferiore (ovvero più dettagliata) rispetto a quella predefinita.

Considerazioni sul servizio di rapporto

Il servizio di rapporto consente di verificare la configurazione della connessione ODBC personalizzata, l'amministrazione dei rapporti consegnati automaticamente ed il mantenimento di alert e rapporti.

- È possibile creare e gestire connessioni a database ODBC esterni.

Per creare una connessione ODBC esterna:

1. Fare clic su Aggiungi connessione.
2. Immettere le informazioni sulla connessione necessarie.

   Nota: se si seleziona Oracle dall'elenco a discesa Driver ODBC, verrà visualizzato il campo Schema in cui è possibile immettere gli oggetti di schema individuali. Immettere almeno uno schema.
3. Fare clic su Salva.
4. Fare clic su Verifica connessione per convalidare le informazioni immesse.

   Viene visualizzato un messaggio di conferma. Le connessioni create verranno visualizzate nell'elenco di connessioni della procedura guidata di progettazione delle query.

Nell'area di memorizzazione degli alert, impostare il totale degli alert memorizzati ed il numero di giorni in cui saranno conservati:

Numero massimo di alert

Definisce il numero massimo di alert conservati dal server di rapporto per la consultazione.

Minimo: 50

Massimo: 1000

Memorizzazione avvisi

Definisce il numero di giorni in cui gli alert vengono conservati, fino al numero massimo possibile.

Minimo: 1

Massimo: 30

Nell'area Configurazioni rapporto, è possibile verificare il nome e il logo dell'azienda, i contenuti dell'intestazione e del piè di pagina, il colore e il tipo di carattere, nonché altre impostazioni dei rapporti PDF.

- Impostare, nell'area Memorizzazione rapporti, i criteri di memorizzazione per ogni tipo di ricorrenza dei rapporti pianificati.
- Impostare la frequenza con cui l'utilità di memorizzazione ricercherà i rapporti da eliminare automaticamente in base a tali criteri. Ad esempio, se l'utilità di memorizzazione dei rapporti viene eseguita giornalmente, verranno eliminati ogni giorno i rapporti con un'età superiore a quella massima specificata.

Considerazioni sul servizio test della regola

Il servizio dei test della regola controlla i test delle regole di correlazione eseguiti da CA User Activity Reporting Module. È possibile impostare i seguenti valori di test della regola:

Limite evento

Definisce il numero di eventi conservati per incidente l'opzione di accumulo è abilitata. Il Limite evento consente di evitare il traffico eccessivo determinato dalla correlazione durante i periodi con un livello di attività elevato. Quando tale limite viene raggiunto, gli eventuali eventi aggiuntivi vengono persi. Ad esempio, se il limite è impostato su 100, una regola può accumulare fino a un massimo di 100 eventi registrati, inclusi l'evento o eventi di iniziali corrispondenti. L'accumulo eventi continua fino al raggiungimento del limite evento, o più generalmente, quando i valori di intervallo o di limite reimpostano la regola.

Numero massimo di test della regola simultanei

Definisce il numero di test della regola che possono essere eseguiti simultaneamente su un solo server CA User Activity Reporting Module.

Considerazioni sulla sottoscrizione

Un sistema di server proxy/client eroga aggiornamenti delle sottoscrizioni. Il primo server installato viene impostato come server proxy di sottoscrizione predefinito; esso contatta periodicamente il server di sottoscrizione CA alla ricerca di aggiornamenti. Le successive installazioni vengono configurate come client di tale server proxy, il quale verrà contattato periodicamente per gli aggiornamenti. In caso di impossibilità di eseguire il contatto, viene registrato un evento con monitoraggio automatico.

Il sistema predefinito consente di ridurre il traffico di rete eliminando la necessità per ogni server di contattare il server di sottoscrizione CA in modo diretto, essendo tuttavia completamente configurabile. Se necessario, è possibile aggiungere server proxy.

È inoltre possibile ridurre ulteriormente il traffico Internet creando server proxy non in linea, che memorizzano localmente le informazioni di aggiornamento e le inviano ai client quando vengono contattati. È possibile supportare eventuali server proxy non in linea, copiando manualmente nel percorso di download del proxy non in linea quanto presente nel percorso del proxy in linea. I proxy non in linea devono essere configurati in ambienti in cui sono presenti server CA User Activity Reporting Module che non possono accedere a Internet o a un server connesso a Internet.

Durante la configurazione del servizio di sottoscrizione, considerare le seguenti informazioni riguardanti alcune impostazioni e le relative interazioni:

Proxy di sottoscrizione predefinito

Definisce il server proxy predefinito per il servizio di sottoscrizione. Questo proxy deve disporre di accesso a Internet. Se non si definiscono altri proxy di sottoscrizione, il server otterrà gli aggiornamenti di sottoscrizione dal server di sottoscrizione CA e scaricherà gli aggiornamenti binari su tutti i client per poi distribuire gli aggiornamenti di contenuto all'archivio utente CA User Activity Reporting Module. Se si definiscono altri proxy, i client contatteranno questo server per gli aggiornamenti nel caso in cui non sia configurato alcun elenco di proxy di sottoscrizione oppure quando l'elenco configurato sarà esaurito. Il valore predefinito è il primo server installato nel proprio ambiente. Tale valore è disponibile soltanto come impostazione globale.

Chiave pubblica

Definisce la chiave utilizzata per testare e verificare la firma degli aggiornamenti. Aggiornando una coppia di chiavi pubblica-privata, il proxy scaricherà l'aggiornamento del valore della chiave pubblica, aggiornandola. Tale valore è disponibile soltanto come impostazione globale.

Importante: Evitare di aggiornare manualmente questo valore.

Proxy di sottoscrizione

Controlla se il server locale è un proxy di sottoscrizione. Se la casella di controllo del proxy di sottoscrizione viene deselezionata, il server corrisponde a un client di sottoscrizione.

Aggiorna ora

Avvia immediatamente un ciclo di aggiornamento su richiesta per il server selezionato. È possibile eseguire un aggiornamento su richiesta per un solo server alla volta. Questa opzione non è disponibile a livello globale. Aggiornare il server proxy di sottoscrizione prima di eseguire tale operazione sul relativo client di sottoscrizione.

Proxy di sottoscrizione in linea

Controlla se il server locale è un proxy di sottoscrizione in linea. Il server di sottoscrizione proxy in linea utilizza l'accesso a Internet per ottenere gli aggiornamenti di sottoscrizione dal server di sottoscrizione CA e distribuirli nell'ambiente CA User Activity Reporting Module. Per specificare un server come proxy di sottoscrizione in linea, selezionare la casella di controllo Proxy di sottoscrizione e l'opzione Proxy di sottoscrizione in linea. Tale valore è disponibile soltanto come impostazione locale.

Proxy di sottoscrizione non in linea

Controlla se il server locale è un proxy di sottoscrizione non in linea. Un proxy di sottoscrizione non in linea è un server che ottiene aggiornamenti di sottoscrizione tramite una copia della directory manuale (usando SCP) da un proxy di sottoscrizione online. I proxy di sottoscrizione non in linea non richiedono l'accesso ad Internet. Per specificare un server come proxy di sottoscrizione non in linea, selezionare la casella di controllo Proxy di sottoscrizione e l'opzione Proxy di sottoscrizione non in linea. Tale valore è disponibile soltanto come impostazione locale.

Nota: per informazioni sulla configurazione della sottoscrizione non in linea, consultare la *Guida all'amministrazione di CA User Activity Reporting Module.*

URL del feed RSS

Definisce l'URL del server di sottoscrizione CA. I proxy di sottoscrizione in linea utilizzano questo URL per accedere al server di sottoscrizione CA e scaricare gli aggiornamenti relativi.

Moduli disponibili per il download

Consente di selezionare tra i moduli disponibili per il download i moduli applicabili all'ambiente CA User Activity Reporting Module. Fare clic su Sfoglia per visualizzare la finestra di dialogo; i moduli selezionati vengono visualizzati nell'elenco Moduli.

I moduli selezionati vengono scaricati dal server di sottoscrizione CA durante gli aggiornamenti di sottoscrizione. È possibile selezionare i moduli per il download a livello globale. Gli altri proxy di sottoscrizione configurati scaricano questi moduli per impostazione predefinita durante l'aggiornamento. È inoltre possibile selezionare i moduli per il download a livello locale per i singoli server proxy e client. In questo modo le impostazioni globali vengono ignorate e nel server specificato vengono scaricati solo i moduli selezionati. I moduli selezionati per i client vengono utilizzati per aggiornare i moduli corrispondenti installati al loro interno. È possibile selezionare un modulo da scaricare per un client non selezionato per il proxy. Il proxy eseguirà il recupero del modulo per il client, senza installarlo su sé stesso.

Nota: se non è già presente, impostare l'URL del feed RSS. Tale impostazione consente al sistema di leggere il feed RSS e, nell'intervallo di aggiornamento successivo, di visualizzare l'elenco dei moduli disponibili per il download.

Moduli selezionati per il download

Visualizza i moduli selezionati nella finestra di dialogo del browser del feed RSS. Il proxy di sottoscrizione predefinito e tutti gli altri proxy in linea scaricano i moduli dal server di sottoscrizione CA durante il processo di aggiornamento. I moduli elencati possono essere i moduli scelti per il download a livello globale, oppure possono riflettere i moduli selezionati per un determinato server a livello locale.

Server proxy HTTP

Controlla se questo server contatta il server di sottoscrizione CA per l'aggiornamento tramite un proxy HTTP, anziché in maniera diretta.

Indirizzo proxy da utilizzare

Consente di specificare l'indirizzo IP completo del proxy HTTP.

Porta

Specifica il numero della porta utilizzata per contattare il proxy HTTP.

ID utente proxy HTTP

Specifica l'ID utente utilizzato per contattare il proxy HTTP.

Password proxy HTTP

Specifica la password utilizzata per contattare il proxy HTTP.

Pianificazione

Specifica l'ora di avvio e la frequenza per la richiesta degli aggiornamenti di sottoscrizione da parte dei server CA User Activity Reporting Module. I server proxy di sottoscrizione in linea (incluso il server proxy predefinito) contattano il server di sottoscrizione CA e i client proxy contattano i server proxy in base a questa pianificazione. La pianificazione può essere impostata globalmente per tutti i server CA User Activity Reporting Module server; può inoltre essere ignorata a livello locale per un server specificato.

Proxy di sottoscrizione per gli aggiornamenti del client

Consente di impostare i proxy contattati, modo round robin, per gli aggiornamenti di prodotti e del sistema operativo da tutti i client o dal client selezionato. È possibile utilizzare le frecce verso l'alto e verso il basso per controllare l'ordine con cui il client contatta i proxy di sottoscrizione. Il client scaricherà gli aggiornamenti dal primo proxy raggiungibile. Se nessuno dei proxy configurati è disponibile, il client contatta il proxy di sottoscrizione predefinito.

Proxy di sottoscrizione per l'aggiornamento dei contenuti

Consente di selezionare i proxy da utilizzare per distribuire gli aggiornamenti dei contenuti all'archivio utente. È possibile selezionare proxy in linea o non in linea. Tale valore è disponibile soltanto come impostazione globale.

Nota: potrebbe essere utile selezionare più di un server come proxy di sottoscrizione per gli aggiornamenti dei contenuti, per ridondanza.

Ulteriori informazioni:

Spazio libero su disco per gli aggiornamenti (a pagina 241)
Informazioni sulle chiavi pubbliche di sottoscrizione (a pagina 242)

Servizio di stato del sistema

È possibile utilizzare il servizio Stato del sistema per ottenere informazioni su un server CA User Activity Reporting Module e controllarlo. È possibile visualizzare lo stato del sistema solo per i singoli server di CA User Activity Reporting Module. Tutte le impostazioni e le opzioni si applicano a livello locale.

Il servizio Stato del sistema comprende le seguenti schede:

- Amministrazione. Controlla i servizi e server host e crea un file di diagnostica di supporto
- Stato. Esamina lo stato e la versione di servizi e processi di sistema
- Eventi di auto monitoraggio. Esamina gli eventi correlati allo stato del sistema e dei componenti

Ulteriori informazioni

Attività di Stato del sistema (a pagina 180)
Creare un file di diagnostica di supporto (a pagina 181)
Riavviare un server host (a pagina 182)
Riavviare i servizi ELM. (a pagina 182)
Controllare lo stato e la versione dei servizi (a pagina 183)
Controllare gli eventi di automonitoraggio dello stato del sistema (a pagina 183)

Attività di configurazione degli adapter CA

I listener locali ricevono e raccolgono eventi nativi da alcuni tipi di risorse tramite vari tipi di adapter CA.

È possibile visualizzare e modificare due tipi di configurazioni di adapter individuali.

- Una configurazione globale si applica a tutte le istanze di un singolo adapter del proprio ambiente, come tutte le istanze SAPI collector,
- mentre una configurazione locale è relativa a un solo host adapter selezionato, come un singolo SAPI collector.

È anche possibile visualizzare gli eventi di automonitoraggio per ogni servizio adapter o host adapter dalle aree di configurazione globali o locali dell'adapter individuale.

Ulteriori informazioni

Modifica di una configurazione adapter globale (a pagina 174)
Modifica di una configurazione adapter locale (a pagina 175)
Visualizzazione degli eventi adapter di automonitoraggio (a pagina 176)
Visualizzazione dello stato degli adapter (a pagina 177)
Considerazioni sul servizio SAPI (a pagina 178)
Considerazioni su iTechnology Event Service (a pagina 180)

Modifica di una configurazione adapter globale

È possibile modificare le configurazioni adapter globale, che sono impostazioni che si applicano a tutte le istanze di un determinato adapter CA nel proprio ambiente. Ad esempio, è possibile apportare modifiche alla configurazione che valgano per tutti i SAPI collector funzionanti nel proprio ambiente. Una configurazione adapter globale *non* ignora le impostazioni adapter locali che differiscono dall'impostazione globale.

Per modificare una configurazione adapter globale

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Raccolta registri.

   Viene visualizzato l'elenco della cartella Raccolta registri.

2. Fare clic sulla cartella Adapter CA.

   La cartella si espande e mostra una sottocartella per ogni adapter.

3. Selezionare la cartella dell'adapter di cui si vuole modificare la configurazione.

   Nel riquadro dei dettagli viene visualizzata la configurazione di servizio globale.

4. Apportare le modifiche desiderate alla configurazione.

   Nota: facendo clic su Ripristina, i valori di configurazione vengono ripristinati allo stato salvato più recente. È possibile annullare una o più modifiche fino a quando si fa clic su Salva. Una volta salvate le modifiche, sarà necessario ripristinarle individualmente.

5. Una volta terminate le modifiche, fare clic su Salva.

   Tutti i cambiamenti apportati alla configurazione vengono applicati a tutti gli host dell'adapter selezionato, a meno che abbiano diverse impostazioni locali.

Modifica di una configurazione adapter locale

È possibile visualizzare o modificare le configurazioni adapter locali. Le configurazioni adapter locali consentono di controllare le impostazioni che potrebbero non applicarsi o essere richieste per l'intero ambiente. Ignorano le impostazioni globali soltanto per host adapter specifici. Ad esempio, potrebbe essere necessario far sì che un host adapter SAPI specifico ascolti su una porta diversa. Questo comportamento può essere impostato con una configurazione locale.

Per modificare una configurazione adapter locale

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Raccolta registri.

   Viene visualizzato l'elenco della cartella Raccolta registri.

2. Fare clic sulla cartella Adapter CA.

   La cartella si espande e mostra una sottocartella per ogni adapter.

3. Selezionare la cartella dell'adapter di cui si desidera modificare la configurazione.

   La visualizzazione del servizio si espande e mostra gli host adapter.

4. Fare clic sull'host adapter desiderato.

   Nel riquadro dei dettagli viene visualizzata la configurazione dell'host.

5. Apportare le modifiche desiderate alla configurazione. In ogni campo di immissione dei valori, menu o controllo della configurazione locale viene visualizzato un pulsante di configurazione locale/globale, che permette di passare da uno stato all'altro.

   Configurazione globale:

   Configurazione locale:

   Fare clic sul pulsante per passare dall'impostazione globale a quella locale e rendere il campo di immissione associato disponibile all'uso. Tale campo di immissione deve sempre essere impostato per la configurazione locale perché l'impostazione abbia effetto; se fosse impostato sulla configurazione globale, per quell'adapter sarebbe attiva l'impostazione globale.

   Nota: un clic su Reimposta permette di visualizzare i valori di configurazione salvati più recenti per tutte le configurazioni disponibili. È possibile annullare una o più modifiche fino a quando si fa clic su Salva. Una volta salvate le modifiche, sarà necessario ripristinarle individualmente.

6. Una volta terminate tutte le modifiche, fare clic su Salva.

Ogni modifica apportata viene applicata soltanto all'host adapter selezionato.

Visualizzazione degli eventi adapter di automonitoraggio

È possibile monitorare le attività del servizio adapter e risolvere i problemi visualizzando gli eventi di automonitoraggio per ogni host servizio adapter. È possibile visualizzare eventi di pre-screening dalle aree di configurazione globale o locale dell'adapter individuale.

Per visualizzare gli eventi di automonitoraggio dell'adapter

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Raccolta registri.

   Viene visualizzato l'elenco della cartella Raccolta registri.

2. Fare clic sulla cartella Adapter CA.

   La cartella si espande e mostra una sottocartella per ogni servizio adapter.

3. Selezionare la cartella perché un servizio adapter possa visualizzare gli eventi di automonitoraggio per quel servizio,oppure espandere le cartelle e scegliere un host adapter per visualizzare soltanto gli eventi di automonitoraggio relativi a quell'host.

   La configurazione dell'adapter viene visualizzata nel riquadro dei dettagli.

4. Fare clic sulla scheda Eventi di automonitoraggio.

   Viene visualizzata una finestra che mostra gli eventi adeguatamente filtrati. Ad esempio, se si seleziona la cartella Plugin evento iTechnology nel passaggio 3, è possibile visualizzare gli eventi di automonitoraggio per tutte le istanze del plugin evento iTechnology. Se si seleziona un host specifico dalla cartella Plugin evento iTechnology, sarà possibile visualizzare soltanto gli eventi relativi a quello specifico host iTechnology.

   Nota: è la propria struttura federata a controllare quali eventi sono visibili. Se non è impostata alcuna federazione, verranno visualizzati solo gli eventi locali, a prescindere dall'host selezionato.

Ulteriori informazioni

Visualizzazione dello stato degli adapter (a pagina 177)
Modifica di una configurazione adapter globale (a pagina 174)
Modifica di una configurazione adapter locale (a pagina 175)

Visualizzazione dello stato degli adapter

È possibile visualizzare lo stato attuale di alcuni servizi adapter CA, tra cui ora di avvio, stato di funzionamento e informazioni e statistiche sul recapito degli eventi. Non si può visualizzare lo stato del servizio plug-in dell'evento iTechnology.

Per visualizzare lo stato di un adapter

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Raccolta registri.

   Viene visualizzato l'elenco della cartella Raccolta registri.

2. Fare clic sulla cartella Adapter CA.

   La cartella si espande e mostra una sottocartella per ogni servizio adapter.

3. Selezionare la cartella dell'adapter di cui si desidera visualizzare lo stato.

   La visualizzazione del servizio si espande e mostra gli host adapter individuali.

4. Fare clic sull'host adapter desiderato.

   Nel riquadro dei dettagli viene visualizzata la configurazione dell'host.

5. Fare clic sulla scheda Stato.

   Vengono visualizzate le informazioni relative allo stato.

   Nota: le informazioni relative allo stato compaiono soltanto nel pannello della configurazione locale.

Considerazioni sul servizio SAPI

CA User Activity Reporting Module utilizza due istanze di un servizio SAPI (Submit Application Programming Interface) CA Audit, una installata come SAPI Collector e l'altra come SAPI Router. Generalmente i servizi SAPI vengono utilizzati per ricevere eventi dai client di controllo CA e dai prodotti integrati. È possibile configurare gli adattatori SAPI tramite le seguenti impostazioni:

Abilita listener

Attiva il servizio selezionato. Questa funzione è attivata per impostazione predefinita.

Porta SAPI

Imposta un numero di porta specifico per il servizio selezionato, a meno che sia registrato con portmapper. Il valore predefinito, 0, consente al servizio di utilizzare una porta specifica in maniera casuale se la casella di controllo Registra è selezionata.

Nota: il numero di porta deve essere diverso per SAPI Collector e SAPI Router. Se per entrambi i servizi è impostata la stessa porta, la seconda impostata non funzionerà/.

Registra

Controlla se il servizio esegue la registrazione con il sistema portmapper. Se si fa clic su Registra e si inserisce 0 nel campo Porta SAPI, verrà selezionata una porta in modo casuale ad ogni avvio del servizio. Questa è l'impostazione predefinita per entrambi i campi. Se la casella Registra non è selezionata, occorre specificare una porta SAPI.

Chiave di crittografia

Definisce la chiave di crittografia nel caso in cui se ne utilizzi una non standard nel proprio ambiente di controllo CA; l'adattatore SAPI la utilizza per leggere gli eventi SAPI in arrivo.

Ordinamento evento

Assicura che gli eventi vengano inviati all'archivio registro eventi nello stesso ordine in cui vengono ricevuti. Se questa opzione è disabilitata, l'ordine può cambiare se alcuni eventi vengono analizzati e inviati più rapidamente di altri. L'abilitazione di Ordinamento evento può influenzare le prestazioni, poiché aumenta le dimensioni della coda di eventi.

Limite eventi

Definisce il numero massimo di eventi nella coda di elaborazione, consentendo il controllo delle risorse di elaborazione. Se si inserisce 0 in questo campo, non si imposta alcun limite. Gli eventi che superano questa soglia verranno ritardati all'origine.

Conteggio dei thread per coda

Definisce il numero di thread di elaborazione per ogni protocollo. L'utilizzo di molti thread di elaborazione rende più veloce l'elaborazione se l'opzione Ordinamento evento è disabilitata. Se invece è abilitata, il conteggio dei thread non avrà effetto. L'utilizzo di molti thread può avere ripercussioni sulle prestazioni.

Crittografie e mapping dei dati

- Il Controllo pilota crittografie determina quali tra le crittografie disponibili sono utilizzate dal servizio per decrittografare i messaggi in arrivo.
- Il Controllo pilota mapping dei dati determina quali tra i file DM disponibili sono utilizzati dal servizio per il mapping degli eventi.

Le impostazioni di registrazione controllano il modo in cui i moduli CA User Activity Reporting Module registrano i messaggi interni. Sono disponibili soltanto come impostazioni locali. Solitamente le impostazioni di registrazione vengono utilizzate per la risoluzione dei problemi. In generale non è necessario modificare queste impostazioni e, comunque, prima di farlo occorre accertarsi di avere una buona conoscenza dei file di registro e della registrazione.

Livello registro

Definisce il tipo e il livello di dettaglio presenti nel file in registrazione. L'elenco a discesa è ordinato per dettaglio: la prima scelta fornisce il minimo di dettaglio e l'ultima il massimo.

Applica a tutti i registratori

Controlla se l'impostazione Livello registro sostituisce tutte le impostazioni di registro dal corrispondente file di proprietà. Quest'impostazione si applica soltanto quando quella di Livello registro è inferiore (quindi mostra più dettagli) dell'impostazione predefinita.

Considerazioni su iTechnology Event Service

iTechnology Event Service controlla gli eventi inviati tramite il daemon iGateway. È possibile configurare il servizio impostando i file DM (Data Mapping) disponibili, che verranno utilizzati dal servizio per il mapping degli eventi tramite il controllo pilota dei file DM.

Il servizio di plug-in degli eventi è preconfigurato per includere la maggior parte dei principali file di mapping dei dati.

Le impostazioni di registrazione controllano il modo in cui i moduli CA User Activity Reporting Module registrano i messaggi interni. Sono disponibili soltanto come impostazioni locali. Solitamente le impostazioni di registrazione vengono utilizzate per la risoluzione dei problemi. In generale non è necessario modificare queste impostazioni e, comunque, prima di farlo occorre accertarsi di avere una buona conoscenza dei file di registro e della registrazione.

Livello registro

Definisce il tipo e il livello di dettaglio presenti nel file in registrazione. L'elenco a discesa è ordinato per dettaglio: la prima opzione fornisce il minimo di dettagli, mentre l'ultima il massimo.

Applica a tutti i registratori

Controlla se l'impostazione Livello registro sostituisce tutte le impostazioni di registro dal corrispondente file di proprietà. Quest'impostazione si applica soltanto quando quella di Livello registro è inferiore (quindi mostra più dettagli) dell'impostazione predefinita.

Attività di Stato del sistema

Nell'ambito del servizio Stato del sistema è possibile eseguire le seguenti operazioni:

- Esaminare lo stato e la versione dei servizi di sistema.
- Esaminare gli eventi di automonitoraggio correlati ai componenti ed all'utilizzo del sistema.
- Creare un file di diagnostica di supporto.
- Riavviare i servizi ELM.
- Riavviare il server host su cui è eseguito il server CA User Activity Reporting Module.
- Abilitare le operazioni in modalità FIPS e non FIPS.

Ulteriori informazioni:

Creare un file di diagnostica di supporto (a pagina 181)
Riavviare un server host (a pagina 182)
Riavviare i servizi ELM. (a pagina 182)
Controllare lo stato e la versione dei servizi (a pagina 183)
Controllare gli eventi di automonitoraggio dello stato del sistema (a pagina 183)

Creare un file di diagnostica di supporto

Si può controllare lo stato della versione dei servizi in esecuzione su un server CA User Activity Reporting Module selezionato. Facendo clic su Diagnostica di supporto verrà eseguito lo script LmDiag.sh disponibile in CA User Activity Reporting Module.

Questa utilità riunisce le informazioni di sistema ed i file di registro in un file compresso .tar che viene trasmesso al personale di supporto di CA. È possibile trasmettere questo file tramite FTP o altro metodo di trasferimento dei file.

Nota: alcune informazioni nel file risultante possono essere riservate, ad esempio gli indirizzi IP, le configurazioni di sistema ed i registri hardware e dei processi. Utilizzare un metodo protetto per memorizzare e trasferire questo file.

Come creare un file di diagnostica

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
2. Espandere la voce Stato di sistema.
3. Selezionare un server specifico di CA User Activity Reporting Module.

   Nella configurazione di servizio dello stato di sistema verrà visualizzata la scheda Amministrazione.
4. Fare clic su Diagnostica di supporto.
5. Selezionare un percorso per il download del file di diagnostica generato.

   Il file verrà creato e scaricato nel percorso specificato. L'utilità verrà chiusa automaticamente una volta copiato il file.

Riavviare un server host

È possibile controllare lo stato e la versione dei servizi in esecuzione su un server CA User Activity Reporting Module selezionato.

Importante: Utilizzare questa funzione solo se necessario o quando viene richiesto dall'assistenza tecnica di CA. Riavviando un server CA User Activity Reporting Module verranno interrotte la ricezione, l'analisi e la memorizzazione dei registri evento fino a quando il riavvio sarà completo. Se si riavvia il server di gestione, sarà necessario chiudere e accedere nuovamente alle sessioni gestite da CA User Activity Reporting Module sugli altri server associati.

Per riavviare un server host

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
2. Espandere la voce Stato del sistema.
3. Selezionare un server CA User Activity Reporting Module.

   Nella configurazione di servizio dello stato di sistema verrà visualizzata la scheda Amministrazione.
4. Fare clic su Riavvia host.

Riavviare i servizi ELM.

È possibile riavviare i servizi ELM in esecuzione sul server CA User Activity Reporting Module selezionato.

Importante: Utilizzare questa funzione solo se necessario o quando viene richiesto dall'assistenza tecnica di CA. Con il riavvio dei servizi ELM, i server CA User Activity Reporting Module non sono più in grado di ricevere, analizzare ed archiviare i log eventi fino al termine del riavvio. Se si riavvia il server di gestione, la sessione corrente e tutte le altre sessioni di CA User Activity Reporting Module su altri server dovranno chiudere la sessione e accedere nuovamente.

Per riavviare i servizi ELM

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
2. Espandere la voce Stato del sistema.
3. Selezionare un server CA User Activity Reporting Module.

   Nella configurazione di servizio dello stato di sistema verrà visualizzata la scheda Amministrazione.
4. Fare clic su Riavvia servizi ELM.

Controllare lo stato e la versione dei servizi

È possibile controllare lo stato della versione dei servizi in esecuzione su un server CA User Activity Reporting Module selezionato.

Per controllare lo stato

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
2. Espandere la voce Stato del sistema.
3. Selezionare un server di CA User Activity Reporting Module specifico.
4. Fare clic sulla scheda Stato.

Controllare gli eventi di automonitoraggio dello stato del sistema

È possibile controllare lo stato della versione dei servizi in esecuzione su un server CA User Activity Reporting Module selezionato. I messaggi di stato contengono gli eventi associati all'utilizzo del processore, dello spazio su disco, delle medie di carico della CPU, della memoria, dell'accesso e dell'utilizzo dell'hardware ed eventi di altro tipo.

Per controllare gli eventi di automonitoraggio

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
2. Espandere la voce Stato del sistema.
3. Selezionare un server di CA User Activity Reporting Module specifico.
4. Fare clic sulla scheda Eventi di automonitoraggio.

Capitolo 6: Archiviazione dei registri

Questa sezione contiene i seguenti argomenti:

Informazioni sull'archiviazione dei log (a pagina 186)
Stati del database del registro eventi (a pagina 188)
Backup e ripristino automatici (a pagina 191)
Controlli di integrità dei dati (a pagina 192)
Configurazione dell'autenticazione non interattiva per il ripristino (a pagina 199)
Invio di query al catalogo archiviazioni (a pagina 205)
Ripristino dei file archiviati automaticamente (a pagina 207)
Script per il ripristino di database archiviati (a pagina 208)
Esecuzione manuale del backup dei database archiviati (a pagina 210)
Ripristino manuale degli archivi dall'archivio registro eventi di origine (a pagina 214)
Ripristino manuale degli archivi dal nuovo archivio registro eventi (a pagina 221)
Monitoraggio di backup e ripristino di LMArchive (a pagina 225)

Informazioni sull'archiviazione dei log

Tramite CA User Activity Reporting Module è possibile gestire due aspetti dell'archiviazione dei log:

- Il backup dei database dei file di log nella directory di archiviazione di ogni server di rapporto su una directory di archiviazione creata dall'utente su un server di archiviazione remoto. Il server di archiviazione remoto è una posizione provvisoria per conservare i database archiviati fino a quando possono essere spostati in una posizione remota.
- Il ripristino dei database dei file di log dalla directory di archiviazione su un server di archiviazione remoto al server di rapporto originale o ad un server CA User Activity Reporting Module definito come punto di ripristino. Una volta eseguito il ripristino, è possibile esaminare i contenuti con query e rapporti.

Si possono gestire i backup dei database dei log eventi scegliendo una delle due modalità seguenti:

- (Metodo consigliato) Configurare CA User Activity Reporting Module per utilizzare l'archiviazione automatica per lo spostamento dei database warm da un server di rapporto CA User Activity Reporting Module ad un server di archiviazione remota in maniera pianificata. Il processo di archiviazione automatica notifica il server di rapporto che è stato eseguito il backup dei database.

  Nota: consultare la sezione Informazioni sull'archiviazione automatica nella *Guida all'implementazione di CA User Activity Reporting Module.*

- Eseguire il backup manuale dei database sul server CA User Activity Reporting Module, quindi copiarli in una posizione di archiviazione on-site. Utilizzare l'utilità LMArchive per richiedere al server CA User Activity Reporting Module di contrassegnare i database come sottoposti a backup.

  Lo spostamento dei file di cui è stato eseguito il backup ad una posizione esterna deve essere eseguito al di fuori di CA User Activity Reporting Module, così come il loro spostamento sulla rete se necessario per il ripristino.

È possibile inviare una query al catalogo dell'archivio per identificare i file dei database da ripristinare. È possibile ripristinare i database in base alle proprie esigenze mediante una delle seguenti due modalità:

- È possibile ripristinarli sul server di rapporto originale scegliendo una delle seguenti due modalità:
  - Se si configura l'autenticazione non interattiva tra il server di archiviazione remoto ed il server di rapporto originale, eseguire lo script restore-ca-elm.sh per ripristinare i database archiviati sul server di rapporto originale.

    Una volta ripristinati i file, interrogarli e creare un rapporto relativo alla durata in giorni configurata per i file warm.
  - Se è stato eseguito il backup manuale dei database di archiviazione, copiare i file nella stessa directory di archiviazione e notificare il ripristino a CA User Activity Reporting Module. Utilizzare un'opzione dell'utilità della riga di comando LMArchive per informare CA User Activity Reporting Module circa il ripristino dei database.

    Una volta ripristinati i file, interrogarli e creare un rapporto relativo alla durata in ore configurata per i file defrosted.
- È possibile ripristinare i database archiviati in un server del punto di ripristino dedicato per esaminare i log di eventi ripristinati attenendosi ad uno dei seguenti metodi:
  - Se si configura l'autenticazione non interattiva dal server di archiviazione remoto nel il punto di ripristino CA User Activity Reporting Module, è possibile eseguire lo script restore-ca-elm.sh per ripristinare i database archiviati nel punto di ripristino.
  - Se l'autenticazione non interattiva non è stata configurata, copiare manualmente i database di archiviazione dal server di archiviazione remoto nella directory di archiviazione del server del punto di ripristino. Quindi, notificare a CA User Activity Reporting Module il ripristino con una ricatalogazione dalla Query di catalogo archiviazioni nella Gestione raccolta log.

    Questa notifica ha come risultato la ricostruzione del catalogo, che rende i file del database disponibili per query e rapporti. La disponibilità dipende dalla durata in giorni configurata per i file warm prima dell'eliminazione impostati su un valore superiore alla durata dei file ripristinati. Di conseguenza, è importante che la durata massima dei file warm venga impostata adeguatamente in ogni punto di ripristino dedicato.

Stati del database del registro eventi

Quando si configura l'archiviazione automatica fra tre server (raccolta, creazione di report, archiviazione remota), tutti i database del registro eventi passano attraverso tre stati: hot, warm e cold. Secondo questa struttura, un database hot di registri non compressi esiste soltanto sul server di raccolta. Il server di rapporto contiene i database warm compressi; il server di archiviazione remota, invece, ospita soltanto i database cold. Quando un database cold viene ripristinato con lo script shell restore, viene ripristinato in stato warm. Quando invece viene ripristinato manualmente con l'utility LMArchive, viene ripristinato in stato defrosted.

I quattro stati dell'archivio registro eventi seguenti descrivono rispettivamente database non compressi, compressi, con backup e trasferimento e ripristinati.

Hot

Lo *stato hot del database* è lo stato del singolo database non compresso dell'archivio registro eventi di un server di raccolta in cui vengono inseriti gli eventi appena elaborati. È possibile configurare il numero massimo di nuovi record da archiviare in un database hot (Numero massimo di righe) prima che venga compresso in un database warm. Si può pianificare l'archiviazione automatica per spostare a ogni ora i database warm dal server di raccolta al server di rapporto configurato (esiste anche un database hot sul server di rapporto, per inserire gli eventi di automonitoraggio).

Warm

Lo *stato warm del database* è quello dei database mantenuti nell'archivio registro eventi del server di rapporto. Se si configura l'archiviazione automatica giornaliera tra il server di rapporto e un server di archiviazione remota, i database warm vengono mantenuti fino a quando non vengono spostati sul server di archiviazione remota. A quel punto, vengono eliminati automaticamente dal server di rapporto. Se non si configura l'archiviazione automatica tra il server di rapporto e un server di archiviazione remota, i database warm possono rimanere sul server di rapporto fino a quando la loro "età" in giorni non raggiunge il valore configurato per Numero massimo di giorni di archiviazione, oppure fino a quando viene raggiunta la soglia dello spazio su disco di archiviazione, a seconda di quale delle due situazioni si verifica prima. Al raggiungimento di una di queste soglie, il database viene eliminato e il suo stato passa a cold. Senza l'archiviazione automatica, è necessario eseguire il backup manuale dei database warm con uno strumento di terze parti prima che vengano eliminati, quindi avviare l'utility LMArchive per notificare a CA User Activity Reporting Module i nomi dei database sottoposti a backup e trasferimento. Lo stato warm viene applicato anche quando si esegue una ricatalogazione con lo script restore-ca-elm.sh o il pulsante Ricataloga dopo il ripristino di un database cold.

Cold

Lo *stato cold del database* si applica ai database sul server di archiviazione remota. La creazione di un record del database cold avviene sul server di rapporto quando il database esegue l'archiviazione automatica al server di gestione remota e viene eliminato dal server di rapporto. Con la gestione manuale, si crea un record del database cold quando l'utility LMArchive viene avviata con l'opzione -notify arch. È possibile interrogare il catalogo dell'archivio di un server di rapporto per identificare i database cold da ripristinare.

Defrosted

Lo *stato defrosted del database* è quello applicato a un database cold fisico che è stato ripristinato nella directory di archiviazione dopo che l'amministratore ha avviato l'utility LMArchive con l'opzione -notify rest per notificare a CA User Activity Reporting Module l'avvenuto ripristino. I database defrosted vengono mantenuti per il numero di ore specificato nel criterio di esportazione.

È possibile interrogare database in qualsiasi stato. Una query normale restituisce dati evento dai database hot e warm sul server di rapporto e dai database defrosted, laddove presenti. Una query federata restituisce dati evento da tutti i server della federazione, tra cui i server di raccolta federati che includono i database hot. Una query di archiviazione restituisce un elenco di database che non esistono più sul server di archiviazione remota utilizzato per l'archiviazione on-site o remota. I database fisici rappresentati da una query di archiviazione possono esistere sul server di archiviazione remota utilizzato per l'archiviazione on-site o remota.

Ulteriori informazioni

Backup e ripristino automatici (a pagina 191)
Esecuzione manuale del backup dei database archiviati (a pagina 210)
Ripristino manuale degli archivi dall'archivio registro eventi di origine (a pagina 214)
Ripristino manuale degli archivi dal nuovo archivio registro eventi (a pagina 221)

Backup e ripristino automatici

Un processo di backup garantisce che nessun dato vada perso durante l'eliminazione dei database precedenti. Il metodo indicato per il backup dei database archiviati consiste nell'utilizzo dell'archiviazione automatica. Si tratta di un trasferimento automatico pianificato di database archiviati eseguito tra coppie di server. L'archiviazione automatica tra un server di origine ed un server di destinazione richiede l'autenticazione non interattiva. L'autenticazione non interattiva utilizza l'autenticazione della chiave pubblica RSA senza passphrase. È possibile configurare l'autenticazione non interattiva e l'archiviazione automatica:

- Da ciascun server di raccolta al relativo server di rapporto.
- Da ciascun server di rapporto al relativo server di archiviazione remoto.

Nota: per ulteriori informazioni, consultare la *Guida all'implementazione*.

Ai fini dell'analisi, un processo di ripristino consente di spostare i database archiviati dall'archiviazione remota ad un server CA User Activity Reporting Module. L'utilizzo dello script restore-ca-elm.sh è il metodo indicato per il ripristino dei database archiviati. Questa utilità di ripristino consente il trasferimento automatico dei database archiviati. Come per il processo di archiviazione automatica, lo script restore-ca-elm.sh utilizza l'autenticazione non interattiva. È possibile configurare l'autenticazione non interattiva ed eseguire lo script di ripristino:

- Dal server di archiviazione remoto a ciascun server di rapporto originale.
- Dal server di archiviazione remoto a ciascun server del punto di ripristino.

Configurare l'esecuzione dell'archiviazione automatica a intervalli regolari. Richiamare il ripristino in base alle esigenze.

Controlli di integrità dei dati

È possibile verificare che gli eventi non elaborati, i dati archiviati o ricatalogati non presentino segni di manomissione effettuando l'accesso come utente con diritti di amministratore. Il controllo verifica che gli eventi non elaborati in arrivo e i dati archiviati non siano stati modificati, consentendo in tal modo il soddisfacimento dei requisiti normativi.

CA User Activity Reporting Module utilizza firme digitali per convalidare database ed eventi non elaborati. Se un database è corrotto, o se la firma di un database è mancante o corrotta, il controllo di integrità dei dati considererà il database modificato. Se la firma per eventi non elaborati è mancante o corrotta, il controllo di integrità dei dati considererà l'evento non elaborato del database come modificato.

CA User Activity Reporting Module consente l'esecuzione di controlli di integrità dei dati per database o eventi non elaborati. Per impostazione predefinita, CA User Activity Reporting Module esegue controlli di integrità dei dati per i database.

Ulteriori informazioni:

Firma dei database in quarantena (a pagina 197)

Funzionamento dei controlli di integrità dei dati per eventi non elaborati

Per eseguire controlli di integrità dei dati per eventi non elaborati, abilitare l'opzione Abilita generazione delle firme per eventi non elaborati. L'attivazione di questa opzione consente di aggiungere un valore alla colonna rawevent_signature per ciascun evento non elaborato ricevuto.

Durante la generazione di un evento non elaborato, CA User Activity Reporting Module esegue una delle seguenti operazioni:

- Se l'opzione Abilita generazione delle firme per eventi non elaborati è abilitata, CA User Activity Reporting Module inserisce il valore della firma dell'evento non elaborato all'evento ed aggiunge l'evento stesso al database.
- Se l'opzione Abilita generazione delle firme per eventi non elaborati è disattivata, CA User Activity Reporting Module aggiunge l'evento al database.

Nota: gli eventi ricevuti con le versioni precedenti di CA User Activity Reporting Module non contengono la colonna rawevent_signature.

Per verificare che il database non contenga entrambi gli eventi (con e senza firma di eventi non elaborati), CA User Activity Reporting Module esegue le seguenti attività indipendentemente dall'attivazione dell'opzione Abilita generazione delle firme per eventi non elaborati.

1. Interruzione di iGateway.
2. Aggiunge il database esistente non elaborato ai database hot.
3. Spostamento dei database hot esistenti per l'archiviazione.

   Nota: quando CA User Activity Reporting Module sposta un database host esistente, la dimensione del database archiviato potrebbe non coincidere con quella del database configurato.
4. Avvio di iGateway.

Ulteriori informazioni:

Attivazione dei controlli di integrità dei dati per eventi non elaborati (a pagina 194)

Attivazione dei controlli di integrità dei dati per eventi non elaborati

Importante: L'esecuzione di controlli di integrità dei dati per eventi non elaborati riduce le prestazioni di CA User Activity Reporting Module a causa di un aumento delle dimensioni del database.

Procedere come descritto di seguito:

1. Fare clic su Amministrazione, Servizi, Configurazione globale.

   Verrà visualizzata la pagina Configurazione di servizio locale: Configurazione globale.

2. Selezionare l'opzione Abilita generazione delle firme per eventi non elaborati nella sezione Integrità dei dati.
3. Fare clic su Salva.

Impostazione dei controlli di integrità dei dati

È possibile impostare i controlli di integrità dei dati nei seguenti modi:

- Automaticamente quando si esegue il ripristino e la ricatalogazione dei dati
- In orari pianificati su server selezionati
- Su richiesta quando è necessario

Nota: è possibile impostare il controllo di integrità dei dati soltanto su richiesta per eventi non elaborati.

È possibile visualizzare i risultati di uno qualsiasi di questi controlli dall'interfaccia Integrità dei dati. Gli eventuali database modificati vengono automaticamente messi in quarantena e visualizzati nell'elenco Database in quarantena. Quando viene eseguito un controllo di integrità dei dati per eventi non elaborati, CA User Activity Reporting Module non mette in quarantena un database contenente eventi modificati. CA User Activity Reporting Module evidenzia soltanto un database modificato e fornisce un'opzione per l'esportazione degli eventi non elaborati modificati del database sul computer locale in formato CSV.gz.

Ulteriori informazioni:

Attivazione del controllo di integrità automatico (a pagina 195)
Pianificazione di un controllo di integrità dei dati (a pagina 195)
Controllo di integrità dei dati su richiesta (a pagina 196)

Attivazione del controllo di integrità automatico

È possibile impostare l'esecuzione automatica del controllo di integrità dei dati ogni volta che si esegue il ripristino o la ricatalogazione dei dati.

Per attivare un controllo automatico di integrità dei dati

1. Fare clic sulla scheda Amministrazione, quindi espandere la sottoscheda Servizi.
2. Selezionare il nodo Deposito eventi di log per attivare l'esecuzione di controlli automatici globali, oppure espandere il nodo Deposito eventi di log e selezionare un server CA User Activity Reporting Module per attivare una verifica automatica locale.
3. Selezionare Convalida integrità su ricatalogazione e ripristino.

Pianificazione di un controllo di integrità dei dati

È possibile pianificare l'esecuzione giornaliera dei controlli di integrità dei dati ad orari impostati e sui server CA User Activity Reporting Module selezionati. Gli eventuali database modificati rilevati da un controllo di integrità pianificato vengono automaticamente messi in quarantena.

Per pianificare un controllo di integrità dei dati

1. Fare clic sulla scheda Amministrazione, quindi espandere la sottoscheda Servizi.
2. Selezionare il nodo Deposito eventi di log per pianificare un controllo globale, oppure espandere il nodo Deposito eventi di log e selezionare un server CA User Activity Reporting Module per impostare una verifica locale.
3. Selezionare Attivato.
4. (Facoltativo) Selezionare Federato per eseguire la verifica pianificata su qualsiasi server federato visibile dal server selezionato.
5. Impostare l'ora di avvio giornaliera.

Controllo di integrità dei dati su richiesta

È possibile eseguire un controllo di integrità dei dati per un database o per eventi non elaborati in qualsiasi momento su un server CA User Activity Reporting Module selezionato.

Per eseguire un controllo di integrità dei dati su richiesta

1. Fare clic sulla scheda Amministrazione e quindi sulla sottoscheda Gestione archivio.
2. Espandere la cartella Integrità dei dati e selezionare il server CA User Activity Reporting Module in cui si desidera eseguire il controllo.
3. Selezionare Database o Eventi non elaborati.
4. Selezionare un intervallo di tempo per il controllo.
5. (Facoltativo) Selezionare Federato per eseguire la verifica su qualsiasi server federato visibile dal server selezionato.
6. Fare clic su Convalida ora.

   CA User Activity Reporting Module visualizza le seguenti informazioni in base al controllo di integrità dei dati selezionato:

   - Un elenco di eventi non elaborati o di database verificati.
   - Il numero di convalide eseguite correttamente e di quelle con errori.
   - Se è stato selezionato Database, il numero di database validi e non validi.
   - Se è stata selezionata l'opzione Eventi non elaborati e il database contiene eventi con la firma di evento non elaborato, CA User Activity Reporting Module convaliderà il database di eventi non elaborati protetti. Se la convalida ha esito positivo, CA User Activity Reporting Module visualizzerà un messaggio di conferma ed aumenterà di un punto il numero di operazioni eseguite correttamente. Se la convalida ha esito negativo, CA User Activity Reporting Module visualizzerà un messaggio di errore, fornirà un'opzione per l'esportazione degli eventi non elaborati modificati sul computer locale in formato CSV.gz, ed aumenterà di un punto il numero di operazioni non riuscite.
   - Se è stata selezionata l'opzione Eventi non elaborati e il database non contiene eventi con la firma di evento non elaborato, CA User Activity Reporting Module rifiuterà il database e visualizzerà un messaggio di errore.

Nota: non è possibile eseguire un controllo dell'integrità dei dati per eventi non elaborati ricevuti da versioni precedenti di CA User Activity Reporting Module r12.5.02.

Firma dei database in quarantena

È possibile rigenerare la firma digitale di un database in quarantena, rendendolo disponibile per le query.

Per rigenerare la firma di un database in quarantena

1. Fare clic sulla scheda Amministrazione e quindi sulla sottoscheda Gestione archivio.
2. Espandere la cartella Integrità dei dati e selezionare il server CA User Activity Reporting Module in cui si trovano i database in quarantena.
3. Fare clic sulla scheda Database in quarantena nel riquadro a destra.
4. Selezionare il database per cui si desidera rigenerare una firma.
5. Fare clic su Genera firma.

   Verrà visualizzato un messaggio di conferma.

Rotazione delle chiavi

È possibile ruotare le chiavi di registrazione utilizzate per proteggere i database archiviati e migliorare così la protezione.

Le chiavi di registrazione utilizzano una combinazione di chiavi di crittografia, una pubblica e una privata, per proteggere i file del database. Quando si ruotano le chiavi, la vecchia chiave pubblica viene conservata, in modo che CA User Activity Reporting Module possa verificare i file che utilizzano la vecchia chiave privata.

Per ruotare le chiavi di registrazione

1. Fare clic sulla scheda Amministrazione, quindi espandere la sottoscheda Servizi.
2. Selezionare la cartella Integrità dei dati e fare clic su Ruota chiavi.

   Viene visualizzato un messaggio di conferma.

Importazione di chiavi

È possibile importare le chiavi di registrazione pubbliche utilizzate per proteggere i database archiviati da un'origine esterna. L'importazione consente di conservare le chiavi utilizzate da altri server CA User Activity Reporting Module precedenti, o da server precedenti. Ad esempio, se si conserva un elenco di backup delle chiavi pubbliche, è possibile eseguirne l'importazione per poter verificare le vecchie firme di database su un server CA User Activity Reporting Module appena creato.

Per importare le chiavi di registrazione

1. Fare clic sulla scheda Amministrazione, quindi espandere la sottoscheda Servizi.
2. Selezionare la cartella Integrità dei dati e fare clic su Importa chiavi.

   Verrà visualizzata la finestra di dialogo di importazione.
3. Individuare il file di chiavi XML da importare e fare clic su OK.

   Viene visualizzato un messaggio di conferma.

   Nota: è possibile importare solo le chiavi in formato XML.

Esportazione di chiavi

È possibile esportare le chiavi di registrazione pubbliche utilizzate per proteggere i database archiviati. L'esportazione consente di eseguire il backup delle chiavi per la successiva importazione in altri server CA User Activity Reporting Module.

Per esportare le chiavi di registrazione

1. Fare clic sulla scheda Amministrazione, quindi espandere la sottoscheda Servizi.
2. Selezionare la cartella Integrità dei dati e fare clic su Esporta chiavi.

   Viene visualizzata la finestra di dialogo di esportazione.
3. Selezionare il percorso desiderato e fare clic su Salva.

Configurazione dell'autenticazione non interattiva per il ripristino

Dopo aver configurato l'autenticazione non interattiva ssh tra il server di archiviazione remoto ed il server di destinazione, è possibile utilizzare lo script shell restore-ca-elm per ripristinare i database archiviati su richiesta. Per il ripristino, il server di archiviazione remoto è il server di origine ed il server di rapporto CA User Activity Reporting Module o il punto di ripristino CA User Activity Reporting Module è il server di destinazione.

I processi si differenziano leggermente in base al tipo di destinazione (server di rapporto o punto di ripristino dedicato).

- Se si utilizza un punto di ripristino dedicato, impostare l'autenticazione non interattiva una sola volta ed utilizzarla per ogni ripristino. La procedura consente di impostare la directory .ssh sul punto di ripristino con la proprietà richiesta e di impostare le autorizzazioni sul file di chiave.
- Se si ripristinano database archiviati dal server di archiviazione remoto a server di rapporto multipli, impostare l'autenticazione non interattiva per ogni coppia di server. Creare la coppia di chiavi una sola volta e copiare la chiave pubblica della coppia per ogni server di rapporto di destinazione. Ad esempio, copiare la chiave pubblica come authorized_keys_RSS dal server di archiviazione remoto per ogni server di rapporto. Per ogni server di rapporto, concatenare il file authorized_keys_RSS al file authorized_keys esistente. Il file esistente contiene le chiavi pubbliche copiate da ciascun server di raccolta.

Entrambi i processi presuppongono la preparazione del server di archiviazione remoto per agire come server di destinazione per l'archiviazione automatica. In tal caso, è richiesta l'autenticazione non interattiva. Se la procedura di preparazione non è stata eseguita, consultare la sezione Creazione di una struttura di directory con proprietà sul server di archiviazione remoto nella *Guida all'implementazione*.

Esempio: Configurazione dell'autenticazione dal server di archiviazione remoto ad un punto di ripristino

L'utilizzo di un server CA User Activity Reporting Module come punto di ripristino facilita l'impostazione dell'autenticazione non interattiva. Dopo aver configurato l'autenticazione tra il server di archiviazione remoto ed il punto di ripristino, è possibile utilizzare lo script restore-ca-elm.sh per ogni ripristino senza ulteriori passaggi per l'autenticazione.

Il processo di configurazione dell'autenticazione non interattiva da un server di archiviazione ad un punto di ripristino CA User Activity Reporting Module prevede le seguenti procedure:

1. Dal server di archiviazione remoto, generare la coppia di chiavi pubblica/privata RSA. Copiare la chiave pubblica come authorized_keys nella directory /tmp sul punto di ripristino.
2. Dal punto di ripristino, creare la directory .ssh in /opt/CA/LogManager ed impostare la proprietà su caelmservice. Copiare authorized_keys dalla directory /tmp alla directory .ssh. Cambiare la proprietà ed impostare le autorizzazioni su authorized_keys.
3. Convalidare le autenticazione non interattive completate tra il server di archiviazione remoto ed il punto di ripristino.

Generazione di chiavi e copia della chiave pubblica nel punto di ripristino

Dal server di archiviazione remoto, generare una coppia di chiavi RSA come utente caelmservice. Quindi, copiare il file di chiave pubblica id_rsa.pub come authorized_keys, nella directory /tmp sul punto di ripristino CA User Activity Reporting Module. Un punto di ripristino è un server dedicato all'analisi dei dati ripristinati.

La struttura della directory /opt/CA/LogManager/directory.ssh deve esistere nel server di archiviazione con la proprietà impostata sull'utente ed il gruppo caelmservice. Contiene il file authorized_keys copiato dai server di rapporto. Quando si genera la coppia di chiavi, salvare id_rsa.pub nella directory /opt/CA/LogManager/ssh.

Per generare la coppia di chiavi pubblica/privata RSA per l'autenticazione tra il server di archiviazione remoto ed il punto di ripristino

1. Accedere via ssh al server remoto per l'archiviazione, usando il nome utente caelmadmin.
2. Commutare gli utenti sull'account root.

   ```
   su –
   ```

3. Commutare gli utenti sull'account caelmservice.

   ```
   su – caelmservice
   ```

4. Come caelmservice, generare una coppia di chiavi RSA .

   ```
   ssh-keygen –t rsa
   ```

5. Premere Invio per accettare il valore predefinito per ognuno dei seguenti prompt:
   - Specificare il file in cui salvare la chiave (/opt/CA/LogManager/.ssh/id_rsa):
   - Immettere la passphrase oppure lasciare il campo vuoto:
   - Immettere nuovamente la stessa passphrase:
6. Modificare la directory in: /opt/CA/LogManager.
7. Modificare i permessi della directory .ssh con il seguente comando:

   ```
   chmod 755 .ssh
   ```

8. Accedere a .ssh, in cui è salvata la chiave id_rsa.pub.

   ```
   cd .ssh
   ```

9. Copiare la chiave pubblica come authorized_keys nella directory /tmp sul server del punto di ripristino.

   ```
   scp id_rsa.pub caelmadmin@<restore_point>:/tmp/authorized_keys
   ```

Preparazione del file di chiave pubblica per l'utilizzo

Creare la directory .ssh sul server del punto di ripristino ed impostare la proprietà su caelmservice. Copiare authorized_keys dalla directory /tmp alla directory .ssh. Impostare la proprietà e le autorizzazioni sul file di chiave pubblica.

Per preparare la chiave pubblica sul server del punto di ripristino per l'autenticazione non interattiva

1. Accedere al server del punto di ripristino CA User Activity Reporting Module mediante ssh come utente caelmadmin.
2. Commutare gli utenti su root.
3. Modificare le directory nella directory CA Enterprise Log Manager.

   ```
   cd /opt/CA/LogManager
   ```

4. Creare la directory .ssh:

   ```
   mkdir .ssh
   ```

5. Modificare la proprietà di .ssh per l'utente ed il gruppo caelmservice:

   ```
   chown caelmservice:caelmservice .ssh
   ```

6. Modificare le directory in: /opt/CA/LogManager/.ssh.
7. Copiare il file authorized_keys da /tmp in .ssh:

   ```
   cp /tmp/authorized_keys .
   ```

8. Modificare la proprietà del file authorized_keys in caelmservice:

   ```
   chown caelmservice:caelmservice authorized_keys
   ```

9. Modificare le autorizzazioni nel file authorized_keys:

   ```
   chmod 755 authorized_keys
   ```

Esempio: Configurazione dell'autenticazione da un server di archiviazione ad un server di rapporto

È possibile ripristinare i database archiviati da un server di archiviazione remoto al server di rapporto originale corrispondente, ovvero il server a partire dal quale i database sono stati archiviati automaticamente. Il vantaggio di questo metodo consiste nel non dover ricatalogare i database di archiviazione CA User Activity Reporting Module. I database dei file di log in fase di ripristino sono già conosciuti al server di rapporto. Se si dispone di più server di rapporto, è necessario configurare l'autenticazione non interattiva tra il server di archiviazione remoto e ogni server di rapporto. Il file authorized_keys esiste nella directory .ssh sul server di rapporto. Il file contiene le chiavi pubbliche di ciascuna coppia di chiavi generata in un server di raccolta che esegue l'archiviazione automatica sul server di rapporto. Creare, pertanto, un file di chiavi autorizzate con un suffisso, quindi concatenare il file al file di origine authorized_keys.

Il processo di configurazione dell'autenticazione non interattiva da un server di archiviazione remoto ad un punto di ripristino CA User Activity Reporting Module prevede le seguenti procedure:

1. Dal server di archiviazione remoto:
   a. Configurare la coppia di chiavi pubblica/privata RSA per l'autenticazione tra il server di archiviazione remota ed il server di rapporto.
   b. Copiare la chiave pubblica come authorized_keys_RSS dal server di archiviazione nella directory /tmp sul server di rapporto.
2. Dal server di rapporto:
   a. Copiare il file authorized_keys corrente da .ssh a /tmp.
   b. Concatenare il file authorized_keys_RSS della directory /tmp nel file authorized_keys.
   c. Copiare il file authorized_keys aggiunto alla directory .ssh.
3. Dal server di archiviazione remoto, convalidare l'autenticazione non interattiva completata tra i server.
4. Ripetere i passaggi per ciascuna combinazione di un server di archiviazione remoto e di un server di rapporto.

Generazione di chiavi e copia della chiave pubblica in un server di rapporto

Dal server di archiviazione remoto, generare una coppia di chiavi RSA come utente caelmservice e copiare la chiave pubblica come file authorized_keys_RSS nella directory /tmp su un server di rapporto CA User Activity Reporting Module. Il server di rapporto include solitamente un file authorized_keys nella directory .ssh contenente una concatenazione di chiavi pubbliche provenienti da vari server di raccolta. Inviare la chiave con un nome univoco, in modo da poter essere aggiunto al file authorized_keys.

Per generare la coppia di chiavi pubblica/privata RSA e copiare la chiave pubblica da un server di archiviazione remoto ad un server di rapporto

1. Accedere al server di archiviazione remoto mediante ssh come utente caelmadmin.
2. Commutare gli utenti su root.
3. Commutare gli utenti sull'account caelmservice.

   ```
   su – caelmservice
   ```

4. Come caelmservice, generare una coppia di chiavi RSA .

   ```
   ssh-keygen –t rsa
   ```

5. Premere Invio per accettare il valore predefinito per ognuno dei seguenti prompt:
   - Specificare il file in cui salvare la chiave (/opt/CA/LogManager/.ssh/id_rsa):
   - Immettere la passphrase oppure lasciare il campo vuoto:
   - Immettere nuovamente la stessa passphrase:
6. Modificare i permessi della directory .ssh con il seguente comando:

   ```
   chmod 755 .ssh
   ```

7. Accedere alla directory .ssh.
8. Copiare id_rsa.pub come authorized_keys_RSS nella directory /tmp sul server di rapporto.

   ```
   scp id_rsa.pub caelmadmin@<reporting_server>:/tmp/authorized_keys_RSS
   ```

Aggiornamento del file di chiave pubblica esistente

È stata copiata la chiave pubblica authorized_keys_RSS nella directory /tmp sul server di rapporto. È ora necessario preparare il file di chiave pubblica esistente. Per eseguire l'operazione, è necessario aggiungere authorized_keys_RSS al file authorized_keys. La proprietà e le autorizzazioni corrette sono già impostate nel file authorized_keys esistente.

Per aggiungere authorized_keys_RSS al file authorized_keys e copiarlo nella posizione corretta

1. Accedere al server di rapporto CA User Activity Reporting Module mediante ssh come utente caelmadmin.
2. Commutare gli utenti su root.
3. Cambiare le directory nella directory /tmp contenente authorized_keys_RSS.
4. Copiare il file authorized_keys esistente da .ssh alla directory corrente /tmp.

   ```
   cp /opt/CA/LogManager/.ssh/authorized_keys
   ```

5. Aggiungere i contenuti della chiave pubblica dal server di archiviazione remoto al file authorized_keys contenente chiavi pubbliche provenienti dai server di raccolta.

   ```
   cat authorized_keys_RSS >> authorized_keys
   ```

6. Modificare le directory in: /opt/CA/LogManager/.ssh.
7. Copiare il file authorized_keys dalla directory/tmp nella directory corrente .ssh:

   ```
   cp /tmp/authorized_keys .
   ```

Invio di query al catalogo archiviazioni

È possibile creare query per ricercare il catalogo di archiviazione locale dei database archiviati in remoto utilizzando filtri rapidi o avanzati. I risultati della query aiutano ad identificare i file di database sottoposti a backup da ripristinare per eseguire un'analisi.

Per inviare una query al catalogo archiviazioni

1. Fare clic sulla scheda Amministrazione e quindi sulla sottoscheda Archival Management (Gestione archivio).

   Viene visualizzato l'elenco cartelle Archival Explorer (Gestione archivio).

2. Fare clic sulla cartella Archival Query (Query archivio) e Ricataloga.

   Nel riquadro dei dettagli viene visualizzata la finestra di dialogo delle query di archiviazione.

3. Selezionare o immettere il periodo di tempo della query.
4. Fare clic su Aggiungi filtro, selezionare una colonna ed inserire il valore di ricerca nella colonna. È possibile aggiungere più filtri.
5. Selezionare Escludi da query per tutti i registri, *ad eccezione* dei registri con il valore inserito dall'utente.

   Nota: se si crea un filtro specificando una colonna che *non* si trova nel catalogo, CA User Activity Reporting Module restituisce tutti i database nell'intervallo di tempo specificato, piuttosto che un set vuoto. Non è necessario conoscere tutte le colonne catalogate per creare una query di archiviazione utile.

6. (Facoltativo) Fare clic sulla scheda Filtri avanzati per aggiungere dei filtri avanzati. Comprendono le informazioni sugli eventi se sussiste la relazione appropriata tra la colonna e il valore immesso. Selezionare una colonna, un operatore, quindi selezionare o inserire un valore. Di seguito vengono riportare le descrizioni dei tipi di operatore:

   Operatori relazionali

   Uguale a, diverso da, minore di, maggiore di, minore o uguale a, maggiore o uguale a.

   Simile

   Comprende le informazioni di evento se la colonna contiene un modello corrispondente al testo immesso dall'utente con il carattere jolly %. L% comprende i valori che cominciano con L. %L% comprende i valori contenenti il carattere L, purché non si tratti del primo o dell'ultimo carattere.

   Non uguale

   Include le informazioni sugli eventi se la colonna non contiene lo schema specificato.

   Nel set

   Include le informazioni di evento se la colonna contiene uno più valori del set delimitato da virgole immesso dall'utente. I valori multipli nel set devono essere separati da virgole.

   Non in set

   Include le informazioni di evento se la colonna contiene uno più valori del set delimitato da virgole immesso dall'utente. I valori multipli nel set devono essere separati da virgole.

   Corrisponde a

   Include le informazioni di evento corrispondenti ad uno o più caratteri immessi, consentendo di eseguire una ricerca per parola chiave.

   Con chiave

   Comprende le informazioni di evento impostate come valore chiave durante la configurazione del server di rapporto. Utilizzare valori chiave per impostare la rilevanza per l'azienda o per altri gruppi organizzativi.

   Senza chiave

   Comprende le informazioni di evento non impostate come valore chiave durante la configurazione del server di rapporto. Utilizzare valori chiave per impostare la rilevanza per l'azienda o per altri gruppi organizzativi.

7. Fare clic su Query.

   Vengono visualizzati i risultati della query. Il file contenente i record corrispondenti ai criteri di query verranno visualizzati con il relativo percorso completo corrispondente a $IGW_LOC. Ecco alcuni esempi:

   ../../LogManager/data/archive/<databaseFilename>

   <remoteHostname>-.../../LogManager/data/archive/<databaseFilename>

Ripristino dei file archiviati automaticamente

Se i file archiviati vengono copiati da un archivio esterno al server remoto configurato per l'archiviazione automatica, è possibile ripristinarli tramite lo script restore-ca-elm.sh. Questa alternativa è da preferirsi all'uso manuale dell'utility LMArchive.

Per ripristinare i file archiviati automaticamente

1. Utilizzare le credenziali caelmadmin per accedere al server CA Enterprise Log Manager con l'archivio registro eventi in cui si desidera ripristinare il database:
2. Al prompt dei comandi, passare all'utente principale, ovvero:

   ```
   su - root
   ```

3. Passare alla directory /opt/CA/SharedComponents/iTechnology con la seguente scorciatoia:

   ```
   cd $IGW_LOC
   ```

4. Quando richiesto dal programma, far passare gli utenti all'account caelmservice.

   ```
   su - caelmservice
   ```

5. Eseguire il comando seguente, dove *userid* e *pwd* sono le credenziali di un account utente CA Enterprise Log Manager con ruolo di amministratore.

   ```
   restore-ca-elm.sh -euser userid -epasswd pwd -rhost hostname -ruser userid -
   rlocation path -files file1,file2,file3...
   ```

   Nota: per consentire a chi non è amministratore di avviare lo script shell restore-ca-elm, creare un ruolo e un criterio personalizzati. Dopodichè, gli utenti a cui verrà assegnato questo ruolo personalizzato potranno specificare le loro credenziali per userid e pwd.

Ulteriori informazioni:

Script per il ripristino di database archiviati (a pagina 208)
Esempio: consentire a chi non è amministratore di gestire gli archivi (a pagina 111)
Backup e ripristino automatici (a pagina 191)

Script per il ripristino di database archiviati

Non è possibile interrogare o creare un rapporto sui dati che risiedono in un database cold su di un server di archiviazione remoto. Per interrogare o creare un rapporto su tali dati, essi dovranno trovarsi in stato warm su un server di CA User Activity Reporting Module. Lo script shell di ripristino, restore-ca-elm.sh, è un'utilità della riga di comando che consente di trasferire uno specifico database cold e la firma digitale corrispondente in un serverCA User Activity Reporting Module e di ripristinarlo in stato warm. È possibile utilizzare l'utilità di ripristino per riportare un database sul server di rapporto originario o su un punto di ripristino dedicato. La configurazione dell'autenticazione non interattiva costituisce un prerequisito per l'esecuzione dello script di ripristino.

Lo script di ripristino viene eseguito dal server CA User Activity Reporting Module su cui si desidera ripristinare i file. L'host remoto identificato nel comando si riferisce al server di archiviazione remoto. I database cold risiedono nella directory di archiviazione del server di archiviazione remoto.

I requisiti per ripristinare i file di database sul server di rapporto originale o sul server del punto di ripristino sono i seguenti:

- La proprietà del file di chiave RSA è impostata sul server remoto.
- caelmservice, sul server remoto, dispone dell'autorizzazione relativa alla cartella /opt/CA/LogManager.

Per ripristinare i file sul server di un punto di ripristino, eseguire le seguenti azioni aggiuntive:

1. Copiare la chiave RSA dal server di archiviazione remoto al server del punto di ripristino
2. Impostare la proprietà del file di chiave RSA sul server del punto di ripristino.

Il formato del comando è il seguente:

```
restore-ca-elm.sh -euser userid -epasswd pwd -rhost hostname -ruser userid -
rlocation path -files file1,file2,file3...
```

-euser *username*

Indica il nome utente di un account CA User Activity Reporting Module con ruolo di amministratore.

-epasswd *pwd*

Indica la password CA User Activity Reporting Module associata al nome utente.

-rhost *host*

Indica il nome o l'indirizzo IP dell'host remoto in cui si trovano i file del database cold nella directory di archiviazione. L'host remoto non è un server CA User Activity Reporting Module.

-ruser remote *user*

Indica l'account utente in possesso delle autorizzazioni per il percorso /opt/CA/LogManager e della proprietà della cartella .ssh contenente il file delle chiavi autorizzate. Di solito, questo account utente è caelmservice.

-rlocation *path*

Indica il percorso dei file di database sul server di archiviazione remoto. Se il server di archiviazione remoto è un server UNIX, il percorso sarà /opt/CA/LogManager/data/archive.

files *file1,file2,file3...*

Specifica un elenco separato da virgole e senza spazi dei file del database da ripristinare.

Esempio: script shell di ripristino

Il seguente comando di esempio viene eseguito dal server CA User Activity Reporting Module su cui devono essere ripristinati i file del database archiviati. Può essere eseguito da un utente in possesso delle credenziali di account Administrator1, calm_r12. Il server remoto su cui vengono trasferiti i database archiviati provenienti dall'archiviazione off-site è denominato NY-Storage-Svr. Questo server remoto è configurato con un account caelmservice, proprietario della cartella .ssh in cui è copiata la chiave pubblica RSA. Questo account gode di massimi privilegi sulla struttura di directory /opt/CA/LogManager. Il comando specifica che i file da ripristinare si trovano nel percorso della directory data/archive del server NY-Storage-Svr ed identifica NY-Storage-Svr_20081206192014.db.cerod come file del database da ripristinare.

```
restore-ca-elm.sh -euser Administrator1 -epasswd calm_r12 -rhost NY-Storage-Svr -
ruser caelmservice -rlocation /opt/CA/LogManager/data/archive -files
NY-Storage-Svr_20081206192014.db.cerod
```

Ulteriori informazioni:

Ripristino dei file archiviati automaticamente (a pagina 207)
Configurazione dell'autenticazione non interattiva per il ripristino (a pagina 199)
Esempio: Configurazione dell'autenticazione dal server di archiviazione remoto ad un punto di ripristino (a pagina 200)
Esempio: Configurazione dell'autenticazione da un server di archiviazione ad un server di rapporto (a pagina 202)

Esecuzione manuale del backup dei database archiviati

CA User Activity Reporting Module crea automaticamente un nuovo database archiviato ogni volta che i dati vengono spostati dall'archivio hot al warm, secondo le proprie impostazioni. Anche se è consigliabile configurare l'archiviazione automatica per trasferire i database warm su un server remoto, è possibile usare i propri strumenti per eseguire backup dei database archiviati e poi avviare l'utility LMArchive per notificare al sistema che l'operazione è stata eseguita.

Si consiglia di eseguire giornalmente il backup dei database, utilizzando il metodo automatico o quello manuale descritto in questa sezione. È importante, perché i file archiviati nel database warm vengono eliminati automaticamente dopo il tempo specificato o quando lo spazio su disco è inferiore alla percentuale definita.

Il backup manuale dei database warm comprende i passaggi seguenti:

1. Identificazione dei database warm non ancora sottoposti a backup.
2. Esecuzione dei backup.
3. Registrazione dei backup.

Ulteriori informazioni

Identificazione dei database non sottoposti a backup (a pagina 211)
Esecuzione dei backup (a pagina 212)
Registrazione dei backup (a pagina 213)

Identificazione dei database non sottoposti a backup

L'utilità LMArchive consente di visualizzare un elenco di database archiviati non ancora contrassegnati come sottoposti a backup. Per ottenere risultati affidabili, l'utilità deve essere eseguita con l'opzione *-notify arch* ogni volta che viene eseguito il backup dei database archiviati.

Importante: Per evitare confusione, si consiglia di notificare i backup completati al server CA User Activity Reporting Module.

Per visualizzare i nomi di tutti i file dei database archiviati correnti non contrassegnati come sottoposti a backup

1. Utilizzare le proprie credenziali **caelmadmin** per accedere al server CA User Activity Reporting Module con il deposito eventi di log contenente i database che devono essere sottoposti a backup per l'archiviazione.
2. Dal prompt dei comandi, commutare gli utenti su root, ovvero:

   ```
   su - root
   ```

3. Modificare la directory in /opt/CA/SharedComponents/iTechnology usando il seguente collegamento:

   ```
   cd $IGW_LOC
   ```

4. Eseguire il comando seguente, dove *username* e *pwd* sono le credenziali di un account utente CA User Activity Reporting Module con ruolo di amministratore.

   ```
   LMArchive -euser username -epassword pwd –list inc
   ```

Esempio: visualizzare tutti i file archiviati correnti di CA User Activity Reporting Module non contrassegnati come sottoposti a backup

Il seguente comando emesso da un amministratore richiede l'elenco di tutti i database warm non contrassegnati come sottoposti a backup.

```
LMArchive -euser Administrator1 -epassword calmr12 -list inc
```

Viene visualizzato un elenco di file archiviati non contrassegnati come sottoposti a backup, espressi in un formato simile a questo:

```
CAELM Archived Files (not backed up):
    calm04_20091206192014.db.cerod
    calm04_20091206192014.db.sig
```

Esecuzione dei backup

Se l'archiviazione automatica non è stata configurata da un server di rapporto CA User Activity Reporting Module a un server di archiviazione remoto non CA User Activity Reporting Module, occorre eseguire manualmente il backup dei database archiviati e trasferirli in una posizione di archiviazione sicura, come un disco o un server separati.

Importante: assicurarsi di eseguire il backup dei database e di trasferirli prima che vengano *eliminati* dal server di rapporto CA User Activity Reporting Module.

I database warm vengono eliminati automaticamente quando viene raggiunto il valore configurato per Numero massimo di giorni di archiviazione, oppure se la percentuale di spazio su disco è al di sotto del valore configurato per Spazio su disco di archiviazione. Per evitare la perdita di dati dai file eliminati, eseguire regolarmente il backup.

Per eseguire manualmente il backup dei database warm

1. Utilizzare le credenziali caelmadmin per accedere al server di rapporto CA User Activity Reporting Module con l'archivio registro eventi che contiene i database di destinazione.
2. Passare all'utente principale, ovvero:

   ```
   su - root
   ```

3. Modificare la directory in: /opt/CA/LogManager/data/archive.
4. Eseguire il backup dei database warm con uno strumento a scelta e spostarli su un server di archiviazione provvisorio on-site o in una posizione esterna per l'archiviazione a lungo termine, secondo le procedure della propria azienda.

Registrazione dei backup

Ogni volta che si esegue il backup di uno o più database archiviati, assicurarsi di registrare tale operazione sul server CA User Activity Reporting Module su cui si è eseguito il backup.

Nota: la mancata registrazione dei backup causa la creazione di rapporti con dati errati quando si utilizza l'utilità LMArchive per elencare i database sottoposti a backup.

Per registrare i backup di database archiviati specifici

1. Utilizzare le proprie credenziali caelmadmin per accedere al server CA User Activity Reporting Module con il deposito eventi di log contenente i database sottoposti a backup.
2. Dal prompt dei comandi, commutare gli utenti su root, ovvero:

   ```
   su - root
   ```

3. Modificare la directory in /opt/CA/SharedComponents/iTechnology usando il seguente collegamento:

   ```
   cd $IGW_LOC
   ```

4. Eseguire il comando seguente, dove *username* e *pwd* sono le credenziali di un account utente CA User Activity Reporting Module con ruolo di amministratore.

   ```
   LMArchive -euser username -epassword pwd –notify arch –files
   file1,file2,file3...
   ```

Esempio: notificare a CA User Activity Reporting Module che alcuni file sono stati sottoposti a backup

Il seguente comando, emesso dall'amministratore denominato Administrator1, notifica il deposito eventi di log di CA User Activity Reporting Module circa l'esecuzione del backup del database warm calm04_20091206192014.db.cerod. I database sottoposti a backup possono essere trasferiti manualmente a un archivio esterno per la memorizzazione a lungo termine.

```
LMArchive -euser Administrator1 -epassword calmr12 -notify arch
-files calm04_20091206192014.db.cerod
```

Viene visualizzata la notifica di archiviazione del file in un formato simile al seguente:

```
Archive notification sent for file calm04_20091206192014.db.cerod...
```

Ripristino manuale degli archivi dall'archivio registro eventi di origine

A volte può capitare di dover ripristinare i file dei database cold per inviare query o rapporti alla directory di archiviazione di un server CA User Activity Reporting Module. Potrebbe essere necessario per analizzare una violazione della protezione o per un'analisi della conformità annuale o semestrale. Le procedure utilizzate dipendono dai due fattori seguenti:

- Se è stata utilizzata l'archiviazione automatica per eseguire il backup dei file da ripristinare;
- Se i file vengono ripristinati sul server di rapporto originale o su un altro server, come un server dedicato al punto di raccolta.

  Se il ripristino avverrà su un server diverso, consultare "Ripristino degli archivi su un nuovo archivio registro eventi".

Se i file vengono ripristinati sul server di rapporto originale, utilizzare le procedure seguenti:

1. Prepararsi a ripristinare i database archiviati identificando i file da ripristinare e determinando la directory di archiviazione.
2. Spostare i database dall'archivio esterno alla directory di archiviazione sul server remoto configurato per l'archiviazione automatica o sul server di rapporto originale.
3. Se i file archiviati sono stati spostati sul server di archiviazione remota configurato per l'archiviazione automatica, accedere al server di rapporto CA User Activity Reporting Module e ripristinare i file archiviati automaticamente dal server di archiviazione remota con lo script restore-ca-elm.sh.
4. Se i file archiviati sono stati spostati nella directory di archiviazione sul server di rapporto CA User Activity Reporting Module originale, ripristinare i file archiviati manualmente tramite l'utility LMArchive.
5. Verificare che il database defrosted possa essere interrogato eseguendo una query che abbia la data di fine corrispondente alla data del database ripristinato ed esaminandone i risultati.

Ulteriori informazioni

Preparazione del ripristino dei database archiviati (a pagina 215)
Trasferimento dei database archiviati su una directory di archiviazione (a pagina 218)
Ripristino dei file archiviati automaticamente (a pagina 207)
Ripristino dei file archiviati manualmente (a pagina 219)
Verifica del ripristino (a pagina 221)

Preparazione del ripristino dei database archiviati

Prima di ripristinare i database archiviati, occorre conoscere:

- I nomi dei filtri da ripristinare
- Il percorso della directory di archiviazione in cui copiare i file recuperati dall'archiviazione remota. Il percorso è sempre /opt/CA/LogManager/data/archive.

È possibile inviare query al catalogo archiviazioni tramite la scheda Amministrazione di CA User Activity Reporting Module, Gestione raccolta log, in cui è possibile specificare filtri semplici o avanzati. Altrimenti, utilizzare l'utilità della riga di comando secondo le modalità riportate di seguito:

Se si dispone già delle informazioni necessarie, saltare questa procedura.

Per preparare il ripristino dei database archiviati

1. Utilizzare le proprie credenziali caelmadmin per accedere al server CA Enterprise Log Manager contenente il deposito eventi di log in cui si desidera ripristinare i database.
2. Dal prompt dei comandi, commutare gli utenti su root, ovvero:

   ```
   su - root
   ```

3. Modificare la directory in /opt/CA/SharedComponents/iTechnology usando il seguente collegamento:

   ```
   cd $IGW_LOC
   ```

4. Identificare i database da ripristinare in un elenco di file che include quelli sottoposti a backup e trasferiti nell'archiviazione esterna. Per visualizzare l'elenco di tutti i file archiviati in questo catalogo archiviazioni, eseguire il comando seguente, dove userid e pwd sono le credenziali di un account utente CA User Activity Reporting Module con ruolo di amministratore.

   ```
   LMArchive -euser userid -epassword pwd -list all
   ```

   Viene visualizzato l'elenco di tutti i file archiviati.

5. (Facoltativo) Se si sta eseguendo il ripristino da backup manuali, determinare la posizione della directory di archiviazione nella quale devono essere copiati i file dell'archivio cold. Eseguire il comando seguente, dove userid e pwd sono le credenziali di un account utente CA User Activity Reporting Module con ruolo di amministratore.

   ```
   LMArchive -euser userid -epassword pwd -list loc
   ```

   Viene visualizzata la directory di archiviazione.

Esempio: visualizzazione di tutti i file archiviati CA User Activity Reporting Module correnti

Il seguente comando, emesso dall'amministratore CA User Activity Reporting Module (Administrator1), richiede un elenco di tutti i database situati nella directory di archiviazione del deposito eventi di log.

```
LMArchive -euser Administrator1 -epassword calmr12 -list all
```

Viene visualizzato un elenco dei file archiviati correnti in un formato simile al seguente:

```
File archiviati CAELM:
    calm04_20091206191941.db.cerod
    calm04_20091206191958.db.cerod
    calm04_20091206192014.db.cerod
    calm04_20091206191941.db.sig
    calm04_20091206191958.db.sig
    calm04_20091206192014.db.sig
```

Esempio: visualizzazione della directory di archiviazione CA User Activity Reporting Module

Il seguente comando, emesso dall'amministratore CA User Activity Reporting Module (Administrator1), richiede la posizione della directory dei database archiviati:

```
LMArchive -euser Administrator1 -epassword calmr12 -list loc
```

Quella che segue è una risposta tipica:

```
Posizione di archiviazione CAELM (host locale):
../../LogManager/data/archive
```

Ulteriori informazioni:

Invio di query al catalogo archiviazioni (a pagina 205)

Trasferimento dei database archiviati su una directory di archiviazione

Se i file archiviati sono stati spostati in una posizione remota, utilizzare le procedure della propria azienda per recuperarli e trasferirli di nuovo in una posizione on-site.

Spostare di nuovo i database nella directory di archiviazione del server CA User Activity Reporting Module originale o di un server remoto configurato per l'autenticazione non interattiva. La directory di archiviazione è: /opt/ca/LogManager/data/archive.

Per spostare un database archiviato da un archivio esterno alla propria rete

1. È possibile spostare i file del database per ripristinarli dall'archivio esterno alla propria rete nei modi seguenti:
   - Se si utilizza l'archiviazione automatica per spostare automaticamente i file archiviati sul server remoto, occorre poi copiarli nuovamente nella directory di archiviazione del server (questo server remoto è già configurato per l'autenticazione non interattiva con il server CA User Activity Reporting Module sul quale devono essere ripristinati i database archiviati).
   - Se non si utilizza l'archiviazione automatica, copiare nuovamente i file archiviati nella directory di archiviazione sul server CA User Activity Reporting Module originale.
2. Procedere con uno dei metodi seguenti, a seconda della posizione dei file archiviati.
   - Se i file archiviati si trovano sul server remoto configurato per l'archiviazione automatica, ripristinare i file archiviati automaticamente con lo script restore-ca-elm.sh.
   - Se i file archiviati si trovano nella directory di archiviazione sul server CA User Activity Reporting Module originale, notificare a CA User Activity Reporting Module che i file archiviati sono stati ripristinati tramite l'utility LMArchive. Una volta ricevuta la notifica, i file ripristinati vengono posti in stato defrosted.

Ulteriori informazioni:

Ripristino dei file archiviati automaticamente (a pagina 207)
Ripristino dei file archiviati manualmente (a pagina 219)

Ripristino dei file archiviati manualmente

Dopo aver ripristinato uno o più database dall'archiviazione a lungo termine alla directory di archiviazione, occorre modificare la proprietà della directory in utente caelmservice prima di notificare a CA User Activity Reporting Module che i database sono stati ripristinati tramite l'utilità LMArchive. I file archiviati di proprietà dell'utente root non sono stati riconosciuti dall'utilità LMArchive.

L'avvio di LMArchive con l'opzione -notify rest modifica lo stato dei file dei database archiviati da cold a defrosted, in modo che siano disponibili per query e rapporti.

Gli amministratori configurano il numero di ore in cui un database archiviato defrosted viene memorizzato prima di venire eliminato automaticamente dalla directory archiviata con l'impostazione Criterio di esportazione sulla configurazione del servizio Deposito eventi di log.

Per ripristinare i file di database archiviati manualmente

1. Utilizzare le proprie credenziali **caelmadmin** per accedere al server CA User Activity Reporting Module con il deposito eventi di log contenente i database ripristinati.
2. Dal prompt dei comandi, commutare gli utenti su root, ovvero:

   ```
   su - root
   ```

3. Modificare le directory con l'estensione /data. Ad esempio:

   ```
   cd /opt/CA/LogManager/data
   ```

4. Assegnare la proprietà della directory di archiviazione (/opt/CA/LogManager/data/archive) all'account caelmservice.

   ```
   chown -R caelmservice:caelmservice archive
   ```

   La proprietà dei file archiviati viene modificata in caelmservice, l'utente del sistema operativo interno, che è un account senza login.

5. Modificare la directory in /opt/CA/SharedComponents/iTechnology usando il seguente collegamento:

   ```
   cd $IGW_LOC
   ```

6. Eseguire il comando seguente, dove *username* e *pwd* sono le credenziali di un account utente CA User Activity Reporting Module con ruolo di amministratore.

   ```
   LMArchive -euser username -epassword pwd –notify rest –files
   file1,file2,file3
   ```

   Viene visualizzata una finestra di conferma del ripristino. CA User Activity Reporting Module "scongela" i file specificati, che assumono lo stato defrosted. I file defrosted vengono mantenuti per il numero di ore configurato. È possibile configurare il mantenimento fino a un massimo di sette giorni.

Nota: è ora possibile inviare query e creare rapporti a fronte dei dati dell'evento contenuti nei file archiviati ripristinati.

Esempio: notificare a CA User Activity Reporting Module che alcuni database sono stati ripristinati.

Il seguente comando, emesso da un utente CA User Activity Reporting Module con ruolo di amministratore, notifica il deposito eventi di log di CA User Activity Reporting Module che il database cold specificato, calm04_20091206192014.db, è stato copiato nella directory di archiviazione.

```
LMArchive -euser Administrator1 -epassword calmr12 -notify rest
-files calm04_20091206192014.db.cerod
```

Viene visualizzata una conferma di ripristino in un formato simile al seguente:

```
Restore notification sent for file calm04_20091206192014.db.cerod
```

Verifica del ripristino

È possibile verificare velocemente che il database ripristinato sia disponibile per essere esaminato eseguendo una rapida query. Le query normali visualizzano i dati provenienti dai database ripristinati negli stati warm e defrosted.

Prendere in considerazione la procedura seguente.

1. Copiare una query di sottoscrizione concepita per visualizzare il tipo di dettaglio dell'evento in possesso del database ripristinato.
2. Proseguire fino al passaggio della procedura guidata Progettazione query in cui si impostano le condizioni dei risultati e inserire un intervallo di date corrispondente ai file dei database appena scongelati.
3. Salvare la query.
4. Eseguire la query.

Ripristino manuale degli archivi dal nuovo archivio registro eventi

A volte potrebbe essere necessario ripristinare i file degli archivi cold a scopo di query o rapporti, come nel caso di un controllo di conformità annuale o semestrale. Se si decide che un server CA User Activity Reporting Module debba funzionare come punto di ripristino per analisi sui dati cold, occorre ricostruire il catalogo ogni volta che si ripristina un nuovo database su questo CA User Activity Reporting Module. Una ricostruzione del catalogo, o ricatalogazione, si rivela necessaria soltanto quando si ripristinano dati su un server diverso da quello su cui è stato generato.

Importante: assicurarsi che l'impostazione Numero massimo di giorni di archiviazione dell'archivio registro eventi di questo server sia adeguata. Altrimenti, i file ripristinati verranno eliminati immediatamente.

La ricatalogazione viene eseguita automaticamente al riavvio di iGateway, se necessario. Se i database sono stati catalogati in modo incompleto prima della chiusura di iGateway, il processo di ricatalogazione si completerà al riavvio di iGateway. Se uno o più database vengono aggiunti alla directory di archiviazione dei database mentre iGateway è chiuso, il processo di ricatalogazione avverrà al successivo avvio di iGateway.

Il ripristino dei file memorizzati da un archivio esterno a un server CA User Activity Reporting Module diverso da quello su cui sono stati sottoposti a backup prevede i passaggi seguenti:

1. Identificazione dei database da ripristinare. Per informazioni, interrogare il catalogo dell'archivio con filtri.
2. Trasferimento dei file identificati nell'archivio cold dall'archivio esterno alla propria rete.
3. Copia dei database copiati sulla directory di archiviazione. Per visualizzare la directory di archiviazione, avviare l'utility LMArchive con l'opzione -list loc.
4. Ricostruzione del catalogo dell'archivio (ricatalogazione).

   La ricostruzione del catalogo dell'archivio per aggiungere un singolo database può richiedere alcune ore. Dopo aver aspettato sufficientemente a lungo il completamento del processo di ricatalogazione, iniziare l'analisi eseguendo query e rapporti sugli archivi eventi dai database ripristinati.
5. Verifica del ripristino con l'invio di una query.

Nota: se un server CA User Activity Reporting Module diventa il punto di ripristino dedicato, assicurarsi che sia escluso dalla federazione.

Ulteriori informazioni:

Trasferimento dei database archiviati su una directory di archiviazione (a pagina 218)
Configurazione del numero massimo di giorni di archiviazione per gli archivi ripristinati (a pagina 223)
Aggiunta di database ripristinati al catalogo (a pagina 224)
Verifica del ripristino (a pagina 221)
Esempio: consentire a chi non è amministratore di gestire gli archivi (a pagina 111)

Configurazione del numero massimo di giorni di archiviazione per gli archivi ripristinati

Quando l'archivio registro eventi viene configurato per un CA User Activity Reporting Module specializzato come punto di ripristino, si consiglia di ignorare l'impostazione globale del numero massimo di giorni di archiviazione e impostare questo valore sul massimo, ovvero 28000. Se il numero di giorni di archiviazione precedenti all'eliminazione relativo ai file dei database archiviati è impostato su un valore inferiore a quello dell'"età" dei file dei database ripristinati, tali file vengono eliminati dal sistema subito dopo essere stati ripristinati allo stato warm.

Nota: questa procedura vale soltanto per i file ripristinati in un nuovo archivio registro eventi.

Per impostare il numero massimo di giorni di archiviazione in base alla durata dei file ripristinati

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
2. Nell'Elenco servizi, espandere la cartella Archivio registro eventi e selezionare il CA User Activity Reporting Module dedicato al punto di ripristino.
3. Fare clic sul pulsante interruttore accanto a Numero massimo di giorni di archiviazione per passare alla configurazione locale e abilitare il campo di immissione.
4. Impostare il campo su un valore in giorni che comprenda i file più datati che verranno ripristinati. Il valore massimo è 28000.
5. Fare clic su Salva.

Aggiunta di database ripristinati al catalogo

Se si copia il database ripristinato direttamente nella directory di archivio di un server diverso da quello in cui è stato generato, ricostruire il catalogo di archivio per aggiungere il database ripristinato.

Non utilizzare la ricatalogazione in nessuno dei casi seguenti:

- Se si utilizza lo script restore-ca-elm.sh per ripristinare un database archiviato. Lo script shell di ripristino esegue la ricatalogazione automaticamente.
- Se si copia il database ripristinato direttamente nella directory di archiviazione del server in cui è stato generato, occorre notificare a CA User Activity Reporting Module l'avvenuto ripristino del database con l'opzione -notify rest di LMArchive.

Il processo di ricatalogazione imposta il database ripristinato sullo stato "warm" e non "defrosted" come con l'opzione -notify rest di LMArchive. Pertanto, verranno seguite le normali regole di archiviazione, anziché il Criterio di esportazione definito nella configurazione del deposito eventi di log.

Per ricreare il catalogo dell'archivio da aggiungere al database ripristinato

1. Fare clic sulla scheda Amministrazione e quindi sulla sottoscheda Archival Management (Gestione archivio).

   Viene visualizzato l'elenco cartelle Archival Management (Gestione archivio).

2. Fare clic sulla cartella Archival Query (Query archivio) e Ricataloga.

   Sopra le schede Filtri rapidi e Filtri avanzati vengono visualizzati tre pulsanti, tra cui Ricataloga.

3. Fare clic su Ricataloga.

   Verrà visualizzato un messaggio di conferma dell'avvenuta operazione. Il database ripristinato viene aggiunto al catalogo con stato warm.

Ulteriori informazioni:

Esempio: consentire a chi non è amministratore di gestire gli archivi (a pagina 111)

Monitoraggio di backup e ripristino di LMArchive

L'utilità della riga di comando *LMArchive* tiene traccia delle operazioni di backup e ripristino dei database warm nell'archivio registro eventi di un server CA User Activity Reporting Module. Utilizzare LMArchive per eseguire una query utile per ottenere l'elenco dei database warm pronti per l'archiviazione. Dopo aver sottoposto a backup i database elencati e averli trasferiti nell'archivio a lungo termine (cold), utilizzare LMArchive per creare un record sul server CA User Activity Reporting Module su cui è stato eseguito il backup del database. Una volta ripristinato un database cold nel suo server CA User Activity Reporting Module originale, utilizzare LMArchive per inviare a CA User Activity Reporting Module una notifica, in modo tale da impostare i file del database cold sullo stato defrosted per la ricezione di query.

Il formato del comando è il seguente:

```
LMArchive -euser username -epassword pwd {-list [loc|all|inc] | -notify
[arch|rest] -files file1,file2,file3...}
```

-euser *username*

Indica il nome utente di un account CA User Activity Reporting Module con ruolo di amministratore.

-epassword *pwd*

Indica la password CA User Activity Reporting Module associata al nome utente.

-list [loc | all | inc]

Richiede un elenco di uno dei seguenti elementi: posizioni delle directory di archivio, nomi di tutti i database warm e cold e nomi dei soli database warm

loc

Richiede la posizione della directory di archivio.

all

Richiede un elenco di tutti nomi di file che si trovano nella directory di archivio dell'archivio registro eventi.

inc

Richiede un elenco incrementale dei nomi dei file del database warm corrente che non risultano ancora archiviati. La richiesta restituirà i nomi dei file non ancora presenti in backup, spostati in archivi esterni e passati allo stato cold. I file passano allo stato cold una volta notificato lo spostamento con il comando di notifica di questa utilità.

-notify [arch | rest]

Notifica all'archivio registro eventi di CA User Activity Reporting Module che i file specificati sono stati sottoposti a backup o ripristinati correttamente.

arch

Notifica all'archivio registro eventi di CA User Activity Reporting Module che i file specificati sono stati sottoposti a backup correttamente.

rest

Notifica all'archivio registro eventi di CA User Activity Reporting Module che i file specificati sono stati ripristinati correttamente.

-files *file1,file2,file3*...

Indica i nomi dei file del database sottoposti a backup o ripristinati.

Ulteriori informazioni:

Informazioni sull'archiviazione dei log (a pagina 186)
Identificazione dei database non sottoposti a backup (a pagina 211)
Registrazione dei backup (a pagina 213)
Preparazione del ripristino dei database archiviati (a pagina 215)
Ripristino dei file archiviati manualmente (a pagina 219)

Capitolo 7: Sottoscrizione

Questa sezione contiene i seguenti argomenti:

Aggiornamento a CA User Activity Reporting Module versione 12.5 attraverso la sottoscrizione (a pagina 227)
Visualizzazione dello stato di sottoscrizione globale (a pagina 229)
Visualizzazione dello stato di sottoscrizione di un server (a pagina 230)
Modifica della configurazione di sottoscrizione globale (a pagina 232)
Modifica della configurazione di sottoscrizione locale di un server (a pagina 233)
Download e selezione dei moduli per la sottoscrizione non in linea (a pagina 235)
Informazioni sugli aggiornamenti su richiesta (a pagina 237)
Spazio libero su disco per gli aggiornamenti (a pagina 241)
Informazioni sulle chiavi pubbliche di sottoscrizione (a pagina 242)
Automonitoraggio degli eventi per la sottoscrizione (a pagina 242)
Applicazione degli aggiornamenti di sottoscrizione agli agenti ed ai connettori (a pagina 248)

Aggiornamento a CA User Activity Reporting Module versione 12.5 attraverso la sottoscrizione

Per eseguire l'aggiornamento di CA User Activity Reporting Module alla versione 12.5, innanzitutto effettuare l'aggiornamento alla versione 12.5 del prodotto Log Manager, quindi aggiornare tutti gli altri moduli CA User Activity Reporting Module, ad esempio Contenuto, Integrazione e Agente. Tutte le attività di aggiornamento vengono eseguite tramite Sottoscrizione.

Importante: Aggiornare il server di gestione CA User Activity Reporting Module prima di installare nuovi server CA User Activity Reporting Module nella rete. In questo modo si garantisce la corretta registrazione dei nuovi server.

Per eseguire l'aggiornamento a CA User Activity Reporting Module versione 12.5

1. Effettuare l'aggiornamento di Log Manager alla versione 12.5.

   Nota: nell'interfaccia utente aggiornata di CA User Activity Reporting Module 12.5, nella scheda Amministrazione, sottoscheda Servizi, sono presenti sia Modulo di sottoscrizione che Servizio di sottoscrizione. In Modulo di sottoscrizione sono riflesse l'interfaccia e la funzionalità precedenti all'aggiornamento 12.5. La presenza del modulo garantisce la corretta comunicazione tra tutti i server CA User Activity Reporting Module durante l'aggiornamento alla versione 12.5. Una volta completato l'aggiornamento alla versione 12.5 del prodotto Log Manager su un determinato server CA User Activity Reporting Module, utilizzare solo Servizio di sottoscrizione per eseguire ogni ulteriore attività di sottoscrizione e modifica di configurazione.

2. Aggiornare tutti gli altri moduli CA User Activity Reporting Module.

   Importante: Dopo aver eseguito il passaggio 1, nell'interfaccia utente aggiornata di CA User Activity Reporting Module 12.5 sono presenti sia Modulo di sottoscrizione che Servizio di sottoscrizione. Utilizzare solo Servizio di sottoscrizione e non Modulo di sottoscrizione per eseguire ogni ulteriore attività di sottoscrizione, incluso questo passaggio. Modulo di sottoscrizione è presente solo per assicurare la corretta comunicazione tra tutti i server CA User Activity Reporting Module durante l'aggiornamento alla versione 12.5; non utilizzarlo per l'esecuzione di funzioni di sottoscrizione successive all'aggiornamento.

3. Se gli aggiornamenti comprendevano moduli Agente o Connettore, installare gli agenti o i connettori aggiornati.

4. Eseguire nuovamente la registrazione dei prodotti di terze parti e di altri prodotti CA, come CA Access Control, che visualizzano i rapporti CA User Activity Reporting Module nelle rispettive interfacce native utilizzando chiamate Open API.

   In tal modo, sarà possibile aggiornare i certificati modificati in questa versione. Per ulteriori informazioni, consultare la *Guida alla programmazione API di CA User Activity Reporting Module*.

Nota: per ulteriori informazioni sull'esecuzione di questi passaggi, vedere *Aggiornamento a CA User Activity Reporting Module versione 12.5 attraverso la sottoscrizione* nelle *Note di rilascio di CA User Activity Reporting Module 12.5*. Consultare le Note di rilascio anche per informazioni sui problemi noti relativi agli aggiornamenti della sottoscrizione.

Ulteriori informazioni:

Applicazione degli aggiornamenti di sottoscrizione agli agenti ed ai connettori (a pagina 248)

Visualizzazione dello stato di sottoscrizione globale

Il Servizio di sottoscrizione scarica e distribuisce nei server CA User Activity Reporting Module i moduli di sottoscrizione selezionati, in base a una pianificazione configurata dall'utente oppure al momento dell'esecuzione di un aggiornamento su richiesta. È possibile visualizzare lo stato di sottoscrizione corrente dei server CA User Activity Reporting Module attraverso il Dashboard di sottoscrizione.

Il Dashboard di sottoscrizione mostra l'avanzamento di qualsiasi aggiornamento un server CA User Activity Reporting Module stia correntemente scaricando o installando. È inoltre possibile visualizzare lo stato di tutti gli aggiornamenti dei contenuti in corso, nonché un elenco di tutti gli aggiornamenti dei contenuti precedentemente installati.

Per visualizzare lo stato globale delle sottoscrizioni

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
2. Fare clic su Servizio di sottoscrizione.

   Viene visualizzata la Configurazione di servizio globale per il Servizio di sottoscrizione, con la scheda Dashboard di sottoscrizione selezionata.
3. Per visualizzare lo stato degli aggiornamenti dei contenuti, esaminare la finestra Stato della sottoscrizione contenuto.

   Se è in corso un aggiornamento dei contenuti, lo stato dell'aggiornamento viene indicato mediante una barra di avanzamento e messaggi di stato. Fare clic sul pulsante Aggiorna per visualizzare l'avanzamento più aggiornato.
4. Per visualizzare un elenco di tutti gli aggiornamenti dei contenuti correntemente installati, fare clic su Sfoglia catalogo.

   Verrà visualizzata la finestra Contenuto. Fare clic su un tipo di contenuto per visualizzare il nome, la data e la versione di tutti gli aggiornamenti associati correntemente installati.

5. Per visualizzare lo stato della sottoscrizione di qualsiasi server CA User Activity Reporting Module, esaminare la finestra Server.

   Se è in corso un aggiornamento in qualsiasi server CA User Activity Reporting Module, nella colonna Avanzamento del server è visualizzata una barra di avanzamento. Fare clic sul pulsante Aggiorna per visualizzare l'avanzamento più aggiornato.

   Nella finestra Server sono inoltre visualizzate informazioni relative a ciascun server CA User Activity Reporting Module, quali:

   Stato

   Mostra lo stato di sottoscrizione di un determinato server CA User Activity Reporting Module. Gli stati di sottoscrizione sono: inattivo, in attesa, download in corso, installazione in corso, completato e non riuscito.

   Messaggio

   Mostra i messaggi relativi allo stato di sottoscrizione di un determinato server CA User Activity Reporting Module.

   Data

   Mostra la data dell'ultima azione di aggiornamento avviata da un determinato server CA User Activity Reporting Module.

Visualizzazione dello stato di sottoscrizione di un server

Il Servizio di sottoscrizione scarica e distribuisce nei server CA User Activity Reporting Module i moduli di sottoscrizione selezionati, in base a una pianificazione configurata dall'utente oppure al momento dell'esecuzione di un aggiornamento su richiesta. È possibile visualizzare lo stato di sottoscrizione corrente di uno specifico server CA User Activity Reporting Module tramite il Dashboard di sottoscrizione globale oppure tramite la finestra Stato locale del server.

Per visualizzare lo stato di sottoscrizione di un server CA User Activity Reporting Module

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
2. Fare clic su Servizio di sottoscrizione.

   Viene visualizzata la Configurazione di servizio globale per il Servizio di sottoscrizione, con la scheda Dashboard di sottoscrizione selezionata.

3. Eseguire una delle seguenti operazioni:

   - Nella finestra Server, esaminare le informazioni sullo stato del server desiderato. Se è in corso un aggiornamento, nella colonna Avanzamento del server è visualizzata una barra di avanzamento. Fare clic sul pulsante Aggiorna per visualizzare l'avanzamento più aggiornato. Nella finestra Server sono inoltre visualizzate informazioni aggiuntive per ciascun server CA User Activity Reporting Module, quali Stato, Messaggio e Data.

   oppure

   - Per informazioni più dettagliate, nella finestra Server fare clic sul nome del server desiderato per aprire la finestra Stato locale dello specifico server. Se è in corso un aggiornamento, nella finestra Stato sono visualizzati una barra di avanzamento e messaggi di stato dell'avanzamento. Fare clic sul pulsante Aggiorna per visualizzare l'avanzamento più aggiornato. Nella finestra Server sono inoltre visualizzate informazioni relative a ciascun server CA User Activity Reporting Module, quali:

     Stato

     Mostra lo stato di sottoscrizione di un determinato server CA User Activity Reporting Module. Gli stati di sottoscrizione sono: inattivo, in attesa, download in corso, installazione in corso, completato e non riuscito.

     Messaggio

     Mostra i messaggi relativi allo stato di sottoscrizione di un determinato server CA User Activity Reporting Module.

     Data

     Mostra la data dell'ultima azione di aggiornamento avviata da un determinato server CA User Activity Reporting Module.

Modifica della configurazione di sottoscrizione globale

Durante la fase di implementazione, è possibile configurare le impostazioni di sottoscrizione globali per l'ambiente in uso. Tutti i server CA User Activity Reporting Module ereditano ed utilizzano tali impostazioni globali, salvo il caso in cui l' amministratore esegua l'override di un'impostazione globale configurando le impostazioni locali per un singolo server CA User Activity Reporting Module.

Per impostazione predefinita, il primo server installato corrisponde al Proxy di sottoscrizione predefinito e tutti i server installati successivamente vengono configurati come client di sottoscrizione. Se nessun altro proxy è configurato o disponibile, il proxy predefinito esegue il download degli aggiornamenti per i client di sottoscrizione.

È possibile modificare le impostazioni globali in qualsiasi momento. Tutti i server ereditano le modifiche apportate, con eccezione dei server configurati localmente per l'override di tali impostazioni.

Le seguenti impostazioni possono essere selezionate e modificate solo a livello globale:

- Proxy di sottoscrizione predefinito
- Chiave pubblica - Versione
- Proxy di sottoscrizione per l'aggiornamento dei contenuti

Per modificare la configurazione di sottoscrizione globale

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
2. Fare clic su Servizio di sottoscrizione.

   Viene visualizzata la Configurazione di servizio globale per il Servizio di sottoscrizione.
3. Fare clic sulla scheda Amministrazione.
4. Esaminare la Configurazione di servizio globale: nel riquadro sulla destra sono disponibili le impostazioni del Servizio di sottoscrizione. Controllare le impostazioni e apportare le eventuali modifiche necessarie.

   Nota: consultare la Guida in linea per i dettagli a livello di campo.
5. Fare clic su Salva.

Ulteriori informazioni:

Modalità di applicazione degli aggiornamenti di sottoscrizione (a pagina 679)

Modifica della configurazione di sottoscrizione locale di un server

Durante l'implementazione della sottoscrizione, è possibile configurare le impostazioni di sottoscrizione globali, quali la pianificazione di sottoscrizione o un elenco di proxy per l'ambiente in uso. Tali impostazioni globali vengono ereditate dai singoli server CA User Activity Reporting Module.

È possibile eseguire l'override delle impostazioni globali configurando le impostazioni locali di un singolo server. Valutare il ruolo di sottoscrizione di un server se si prevede di eseguire l'override delle impostazioni globali.

Per modificare la configurazione di sottoscrizione di un server

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
2. Espandere il servizio di sottoscrizione e selezionare il server da configurare.

   Viene visualizzata la configurazione del Servizio di sottoscrizione per il server CA User Activity Reporting Module selezionato.
3. Fare clic sulla scheda Amministrazione.
4. Se si desidera modificare il ruolo di sottoscrizione del server, eseguire una delle seguenti operazioni:
   - Per specificare il ruolo di client di sottoscrizione, deselezionare la casella di controllo del proxy di sottoscrizione
   - Per specificare il ruolo come proxy di sottoscrizione in linea, selezionare la casella di controllo del proxy di sottoscrizione e selezionare Proxy di sottoscrizione in linea.
   - Per specificare il ruolo come proxy di sottoscrizione non in linea, selezionare la casella di controllo del proxy di sottoscrizione e selezionare Proxy di sottoscrizione non in linea.

Nota: prima di procedere alla modifica del ruolo di un server da proxy di sottoscrizione a client di sottoscrizione, verificare le configurazioni dei client di sottoscrizione che utilizzano tale proxy. Se si modifica un server da proxy in client, rimuovere immediatamente il server dagli elenchi globali e locali Proxy di sottoscrizione per gli aggiornamenti del client.

Importante: Prima di modificare il ruolo del server in proxy di sottoscrizione non in linea, verificare se è incluso un elenco di proxy. In un ambiente di sottoscrizione misto, con proxy di sottoscrizione in linea e non in linea, non includere i proxy non in linea nell'elenco dei proxy per i client di sottoscrizione in linea.

5. Per eseguire l'override di un'impostazione globale ereditata, fare clic sul pulsante globale/locale per passare alla configurazione di servizio locale per il campo selezionato.

   Nota: per ripristinare l'impostazione globale, fare nuovamente clic sul pulsante. L'impostazione globale verrà ripristinata al momento dell'avvio del successivo aggiornamento.

6. Se i moduli che si desidera scaricare per il server sono diversi dalle impostazioni ereditate dalle impostazioni globali, modificare la configurazione in locale, fare clic su Sfoglia e selezionare i moduli desiderati.

   Nota: verificare che i moduli selezionati per il proxy di sottoscrizione includano tutti i moduli selezionati negli elenchi di download dei client che ricevono gli aggiornamenti da tale proxy.

7. Se il server deve scaricare gli aggiornamenti della sottoscrizione attraverso un server proxy HTTP diverso da quello ereditato, passare alla configurazione locale e configurare il proxy HTTP desiderato.

8. Se il server è configurato per eseguire il download degli aggiornamenti in base a una pianificazione diversa da quella ereditata, passare alla configurazione locale e modificare la pianificazione.

9. Se il server è configurato per eseguire il download degli aggiornamenti da un altro proxy di sottoscrizione CA User Activity Reporting Module, passare alla configurazione locale e aggiungere i server proxy CA User Activity Reporting Module desiderati all'elenco Proxy di sottoscrizione per gli aggiornamenti del client.

   Questo server contatterà i server proxy specificati per il download degli aggiornamenti di sottoscrizione, creando una struttura proxy a livelli.

10. Fare clic su Salva.

Download e selezione dei moduli per la sottoscrizione non in linea

I file di aggiornamento della sottoscrizione non in linea sono disponibili sul sito FTP di sottoscrizione non in linea di CA, sotto forma di file .zip. Non appena disponibili, i nuovi moduli verranno visualizzati sul sito FTP. Controllare regolarmente l'elenco dei moduli disponibili per verificare di aver eseguito il download degli aggiornamenti più recenti. Inoltre è possibile consultare il sito del supporto tecnico di CA all'indirizzo http://ca.com/support per verificare se sono disponibili versioni e service pack nuovi per Gestione log.

Per poter selezionare i moduli da scaricare per i proxy di sottoscrizione non in linea, eseguire il download del pacchetto file di aggiornamento non in linea dal sito FTP di CA e copiarlo manualmente sui proxy non in linea. È quindi possibile selezionare i moduli da scaricare e installare. Al contrario, i client di sottoscrizione non in linea ricevono gli aggiornamenti installati manualmente sui proxy non in linea corrispondenti in modo automatico, indipendentemente dai moduli selezionati per il client a livello locale.

Per scaricare e selezionare i moduli di sottoscrizione non in linea

1. Su un sistema con accesso a Internet o a FTP, accedere al sito FTP di sottoscrizione non in linea:

   ftp://ftp.ca.com/pub/elm/connectors/ftp/outgoing/pub/elm/ELM_Offline_Subscription

   L'indice delle directory visualizza una cartella per ciascuna versione principale di CA User Activity Reporting Module.

2. Scaricare il file .zip corrispondente all'aggiornamento che si desidera eseguire.

   Nota: La cartella della versione r12.5 di CA User Activity Reporting Module contiene una sottocartella e il file .zip. La sottocartella contiene i moduli per l'aggiornamento da una versione precedente alla versione r12.5. Il file .zip contiene i moduli per l'esecuzione degli aggiornamenti periodici regolari alla versione r12.5. Se si utilizza la sottoscrizione non in linea per l'aggiornamento da una versione precedente alla versione r12.5, consultare l'argomento Aggiornamento a CA User Activity Reporting Module delle *Note di rilascio*. Se si sta eseguendo un aggiornamento di routine, selezionare il file .zip.

3. Utilizzare un supporto fisico, ad esempio un disco, oppure l'utilità SCP, per copiare manualmente il file .zip nel seguente percorso del proxy non in linea:

   /opt/CA/LogManager/data/subscription/offline.

4. Accedere a un sistema dell'ambiente CA User Activity Reporting Module.
5. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
6. Espandere Servizio di sottoscrizione e selezionare il server proxy non in linea che si desidera configurare.

   Viene visualizzata la finestra di configurazione del Servizio di sottoscrizione per il server CA User Activity Reporting Module selezionato.

   Nota:i client di sottoscrizione non in linea ricevono automaticamente i moduli installati manualmente sul proxy non in linea corrispondente. Il contenuto del server proxy controlla gli aggiornamenti ricevuti dal client di sottoscrizione. I moduli selezionati a livello locale per un client non in linea non vengono considerati.

7. Fare clic sulla scheda Amministrazione.
8. Nell'elenco a discesa File, selezionare il file di aggiornamento non in linea .zip copiato sul server e fare clic su Sfoglia.

   Viene visualizzata la finestra di dialogo Moduli disponibili per il download.

9. Selezionare i moduli da scaricare.
10. Fare clic su OK.

    La finestra di dialogo Moduli disponibili per il download viene chiusa e i moduli selezionati vengono visualizzati nell'elenco Moduli selezionati per il download.

11. Fare clic su Salva.

    I client di sottoscrizione non in linea possono quindi eseguire il download automatico dei moduli in base al tipo sottoscrizione impostato oppure richiedendo di specificarlo al momento dell'avvio dell'aggiornamento manuale.

12. (Facoltativo) Fare clic su Aggiorna ora.

    L'aggiornamento del server proxy non in linea include solo i moduli selezionati.

    Nota: sebbene il proxy non in linea possa eseguire l'aggiornamento automatico in base al tipo di sottoscrizione impostato, in caso di trasferimento di file nuovi si consiglia di eseguire l'aggiornamento manuale. Questa procedura consente garantire la disponibilità degli aggiornamenti in caso di richiesta da parte dei client di sottoscrizione non in linea.

Informazioni sugli aggiornamenti su richiesta

La differenza fra un aggiornamento su richiesta ed un aggiornamento pianificato consiste nel fatto che il primo viene eseguito immediatamente ed aggiorna soltanto il server selezionato. È possibile richiamare un aggiornamento su richiesta per un solo server CA User Activity Reporting Module alla volta. Prima di eseguire un aggiornamento su richiesta su un client di sottoscrizione, aggiornare il server proxy.

Solitamente, gli aggiornamenti pianificati consentono di mantenere i server di CA User Activity Reporting Module aggiornati con i file binari più recenti e il server di gestione aggiornato con i file di configurazione e di contenuto più recenti. Si consiglia, tuttavia, di richiamare periodicamente un aggiornamento fuori pianificazione su un singolo server.

Valutare l'utilizzo degli aggiornamenti su richiesta per i seguenti casi:

- Viene segnalato un errore o un avviso di evento di sottoscrizione relativo al server di gestione, ad esempio:

  ```
  Impossibile connettersi ad EEMServer.
  ```

  ```
  Errore nell'istallazione dei contenuti in EEM
  ```

  Selezionare il server di gestione e fare clic su Aggiorna ora. Se il server di gestione è configurato come proxy per gli aggiornamenti di contenuto, gli aggiornamenti verranno scaricati dal server di sottoscrizione CA. Successivamente, il server invia gli aggiornamenti di contenuto al repository di contenuto. Se il server è configurato come proxy per i client, è possibile eseguire gli aggiornamenti binari per i relativi client secondo l'ordine cronologico delle richieste.

  Nota: in alternativa, è possibile attendere la sessione di aggiornamento successiva, in cui verranno ripristinati e completati i processi incompleti.

- Un messaggio di errore nell'evento di sottoscrizione indica che il download è stato interrotto. Se il download viene interrotto su un solo server proxy, sarà possibile riprovare ad eseguire il download eseguendo un aggiornamento su richiesta. Se l'errore viene individuato tempestivamente, si consiglia di eseguire un aggiornamento su richiesta. Se l'ora di inizio fra il proxy ed il client è sufficiente, è possibile completare un aggiornamento del proxy su richiesta prima che inizi l'aggiornamento pianificato da parte dei client che ottengono gli aggiornamenti da tale proxy.

- Viene installato un nuovo CA User Activity Reporting Module e configurato come proxy. Prima di utilizzarlo si desidera verificare che vengano applicati gli aggiornamenti più recenti.

- Un modulo richiesto da un client non è selezionato come modulo da scaricare. Tuttavia, tale modulo è stato selezionato come modulo da scaricare da parte del proxy. Eseguire Aggiorna ora sul client per installare gli aggiornamenti mancanti.

- Un pacchetto di sottoscrizione non in linea è stato scaricato e copiato su un proxy di sottoscrizione non in linea. Eseguire un aggiornamento manuale sul proxy se si esegue il trasferimento di file nuovi per garantire che gli aggiornamenti siano disponibili in caso di richiesta da parte dei client di sottoscrizione non in linea.

Avviare un aggiornamento su richiesta

La funzione Aggiorna ora consente di eseguire l'aggiornamento su richiesta di uno o più server. Al momento di aggiornare due o più server in serie, attendere il termine dell'elaborazione su un server prima di avviarla su un altro. Controllare lo stato degli eventi con monitoraggio automatico

Se i valori di sottoscrizione sono stati modificati di recente, attendere la scadenza dell'intervallo di aggiornamento (300 secondi, per impostazione predefinita) prima di eseguire un aggiornamento su richiesta. In CA User Activity Reporting Module è possibile generare un evento di monitoraggio automatico una volta terminato l'aggiornamento.

Nota: nel caso in cui un aggiornamento pianificato sia in esecuzione, il comando Aggiorna ora non apporta alcuna modifica. Se l'ora di inizio di un aggiornamento coincide con l'elaborazione di Aggiorna ora, il processo pianificato non verrà eseguito. Al termine dell'elaborazione su richiesta, verrà ripristinato il ciclo di aggiornamento pianificato.

Importante: Se i moduli che si desidera scaricare contengono aggiornamenti dei contenuti, aggiornare il proxy del contenuto prima di eseguire un aggiornamento su richiesta.

Per aggiornare un server su richiesta

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
2. Espandere Servizio di sottoscrizione in Elenco servizi.
3. Selezionare il server di proxy per gli aggiornamenti di contenuto ed esaminare i moduli selezionati per il download. Se contengono aggiornamenti di contenuti, fare clic su Aggiorna ora.

   Il server recupera gli aggiornamenti dal server di sottoscrizione CA. Trattandosi di un proxy per gli aggiornamenti di contenuto, gli aggiornamenti vengono inviati al repository di contenuto. Trattandosi di un proxy in linea, vengono scaricati gli aggiornamenti binari.
4. Selezionare il server da aggiornare ed esaminarne il ruolo.
5. Se si tratta di un proxy di sottoscrizione per gli aggiornamenti client, fare clic su Aggiorna ora.

   Il server viene aggiornato con i moduli selezionati per il download.

6. Se si tratta di un client con un proxy in linea, eseguire le operazioni riportate a continuazione:
   a. Identificare un proxy per il client tra gli elementi selezionati nell'elenco Proxy di sottoscrizione per il client.
   b. Selezionare il proxy per il client e fare clic su Aggiorna ora.
   c. Selezionare il client e fare clic su Aggiorna ora.

   Il server viene aggiornato con i moduli selezionati per il download.
7. Se si tratta di un proxy di sottoscrizione non in linea, eseguire le operazioni riportate a continuazione:
   a. Scaricare il pacchetto di aggiornamento non in linea dal sito FTP di sottoscrizione non in linea di CA.
   b. Copiare manualmente gli aggiornamenti nel percorso di download del proxy non in linea.

      .../data/subscription/offline
   c. Selezionare il proxy non in linea e il file .zip di aggiornamento non in linea, quindi fare clic su Sfoglia e selezionare i moduli desiderati.
   d. Fare clic su Aggiorna ora.

   Il server viene aggiornato con i moduli selezionati per il download.
8. Se si tratta di un client con un proxy non in linea, eseguire le operazioni riportate a continuazione:
   a. Aggiornare il proxy non in linea come indicato al passaggio 7.
   b. Selezionare il client e fare clic su Aggiorna ora.

   Il server viene aggiornato con tutti i moduli installati sul proxy non in linea corrispondente.

   Nota:i client di sottoscrizione non in linea ricevono automaticamente i moduli installati manualmente sul proxy non in linea corrispondente. I moduli selezionati a livello locale per un client non in linea non vengono considerati.

Spazio libero su disco per gli aggiornamenti

La pulizia regolare del disco garantisce la corretta esecuzione degli aggiornamenti di sottoscrizione sui server CA User Activity Reporting Module. Se all'inizio della procedura di aggiornamento della sottoscrizione lo spazio disponibile sul disco è inferiore a 5 GB, il Servizio di sottoscrizione emetterà un evento di monitoraggio automatico e sospende il processo di download.

Per garantire sufficiente spazio sul disco per gli aggiornamenti di sottoscrizione

1. Monitorare regolarmente lo spazio libero su disco. In alternativa, è possibile impostare un avviso per ricevere una notifica quando lo spazio disponibile sul disco è inferiore al valore specificato.
2. Liberare spazio sul disco con uno strumento di pulizia.
3. Se un evento di monitoraggio automatico segnala la necessità di una pulizia, liberare spazio sul disco a sufficienza per consentire il download.

Ulteriori informazioni:

Esempio: creazione di un avviso per Spazio su disco insufficiente (a pagina 479)

Informazioni sulle chiavi pubbliche di sottoscrizione

Il proxy di sottoscrizione conserva un insieme di chiavi pubbliche corrispondenti alle chiavi private utilizzate dal server di sottoscrizione CA. Il proxy di sottoscrizione esegue il download degli aggiornamenti di sottoscrizione in formato zip con firma digitale utilizzando una chiave privata. L'aggiornamento identifica la chiave pubblica da utilizzare per controllare la firma dell'aggiornamento. La verifica della firma è il metodo con cui il proxy di sottoscrizione si assicura che l'aggiornamento provenga dal server di sottoscrizione CA. Per la sottoscrizione viene utilizzata solo una coppia di chiavi pubbliche-private. La chiave privata viene utilizzata per la firma dell'aggiornamento; la chiave pubblica viene utilizzata per la verifica della firma. La chiave pubblica viene memorizzata in ciascun server CA User Activity Reporting Module e può essere aggiornata.

CA User Activity Reporting Module memorizza la versione iniziale della chiave pubblica nel file di configurazione della sottoscrizione al momento dell'installazione. Nel caso in cui fosse necessaria una nuova chiave privata, il download della chiave pubblica associata viene eseguito con l'aggiornamento della sottoscrizione precedente al ciclo di aggiornamento che richiede la nuova chiave.

Importante: Non eseguire l'aggiornamento manuale del campo Chiave pubblica per la sottoscrizione se non espressamente specificato dal Supporto tecnico di CA.

Automonitoraggio degli eventi per la sottoscrizione

È possibile monitorare i successi e i fallimenti dei processi degli aggiornamenti di sottoscrizione che riguardano i server CA User Activity Reporting Module configurati come segue:

- Proxy di sottoscrizione predefinito
- Proxy di sottoscrizione in linea aggiuntivo, se presente
- Proxy di sottoscrizione non in linea, se presente
- Client di sottoscrizione

Nota: gli eventi qui descritti non tengono traccia degli aggiornamenti di sottoscrizione per gli agenti.

Vengono segnalate le seguenti operazioni correttamente completate:

- Avvio e spegnimento dei server CA User Activity Reporting Module, di entrambi i proxy di sottoscrizione e dei client di sottoscrizione.
- Download riuscito per un componente proveniente da un proxy di sottoscrizione in linea o non in linea che viene scaricato su un client di sottoscrizione.
- Installazione di un componente da parte del client di sottoscrizione riuscita.

Vengono creati rapporti per fallimenti ed errori nei casi seguenti:

- Download non riuscito per un componente proveniente da un proxy di sottoscrizione in linea o non in linea che viene scaricato su un client di sottoscrizione.
- Installazione non riuscita di un componente da parte di un client di sottoscrizione.
- Condizioni di errore

Monitoraggio degli eventi di sottoscrizione

Per monitorare i processi di aggiornamento delle sottoscrizioni riusciti e non riusciti, visualizzare gli eventi con monitoraggio automatico per la sottoscrizione.

Per monitorare i processi degli eventi di sottoscrizione

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
2. Fare clic su Servizio di sottoscrizione in Elenco servizi.
3. Fare clic sulla scheda Eventi con monitoraggio automatico per il servizio di sottoscrizione o per un host elencato in Servizio di sottoscrizione.

4. Esaminare i dettagli dell'evento visualizzati.

   Alcuni dei campi visualizzati per gli eventi di automonitoraggio rispecchiano la modalità CEG standard per fare riferimento alle azioni comuni tra i fornitori. Il Modello ideale si basa su questa gerarchia: event_category, event_class (all'interno la categoria), event_action (all'interno della classe), event_result ed event_severity. Il Livello di gravità CA visualizzato in questo rapporto corrisponde all'interpretazione data da CA alla gravità.

   Gravità CA

   La gravità dell'evento, che può essere:

   - Sconosciuta: eventi sconosciuti, eventi non mappati per CEG o eventi non classificati.
   - Informativa: informazioni sulle operazioni di sistema generali, informazioni relative alla sicurezza, o una notifica.
   - Di avviso: cambiamenti insoliti, una condizione normale ma significativa, operazioni non riuscite o prestazioni degradate.
   - A impatto minimo: impatto minimo per un sistema, una funzione o una protezione.
   - A impatto massimo: impatto massimo per un sistema, una funzione o una protezione.
   - Critica: è richiesto un intervento immediato; probabile violazione della protezione.

   Data

   Quando si è verificato l'evento.

   Destinatario

   Il componente che non è riuscito a completare correttamente il processo corrente. Può trattarsi di un proxy o di un client di sottoscrizione. Se è un proxy di sottoscrizione, può trattarsi del proxy predefinito, di uno in linea o di uno non in linea.

   Host ricevente

   Il nome host del server CA User Activity Reporting Module ricevente.

   Categoria

   La categoria dell'evento. Gestione configurazione è event_category per gli eventi del servizio di sottoscrizione.

Utente

Il nome utente o l'identità che ha inizializzato l'azione espressa nelle informazioni evento. Nella CEG, corrisponde al campo source_username.

Azione

L'azione che ha causato la generazione dell'evento. Nella CEG, corrisponde al campo event_action.

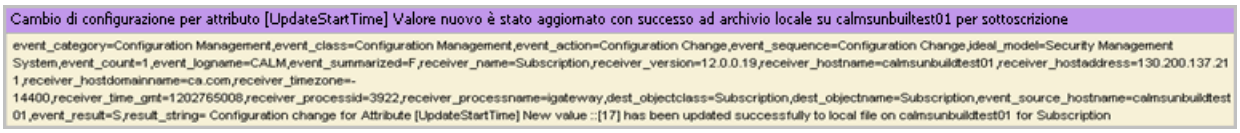
Risultato

S per Successo; F per Fallimento. Il risultato dell'azione evento corrisponde al campo event_result nella CEG. Altre azioni sono Accetta, Rifiuta, Rimuovi e Sconosciuto.

Descrizione risultato

Il testo del messaggio. Se la colonna Risultato contiene Operazione non riuscita, visualizzare il testo Descrizione risultato.

5. Visualizzare i dettagli nel Visualizzatore eventi. Da questo punto è possibile visualizzare modifiche come quelle apportate a un valore della configurazione, come l'ora di inizio aggiornamento.



Visualizzazione dei dettagli degli eventi di sottoscrizione

Una volta configurata la sottoscrizione, è possibile visualizzare gli eventi di automonitoraggio. Dopo un aggiornamento della sottoscrizione è possibile verificare che l'aggiornamento di ogni server sia stato completato correttamente. Durante il completamento degli aggiornamenti, cercare i seguenti messaggi degli eventi di automonitoraggio su ogni server interessato:

- <componente> è stato scaricato correttamente su <nomeproxy> ed installato in EEM.
- <componente> è stato scaricato correttamente sul proxy <nomeproxy>.
- <componente> è stato installato correttamente sul client <nomeclient>.

È anche possibile visualizzare gli eventi di automonitoraggio delle sottoscrizioni a scopo di risoluzione dei problemi.

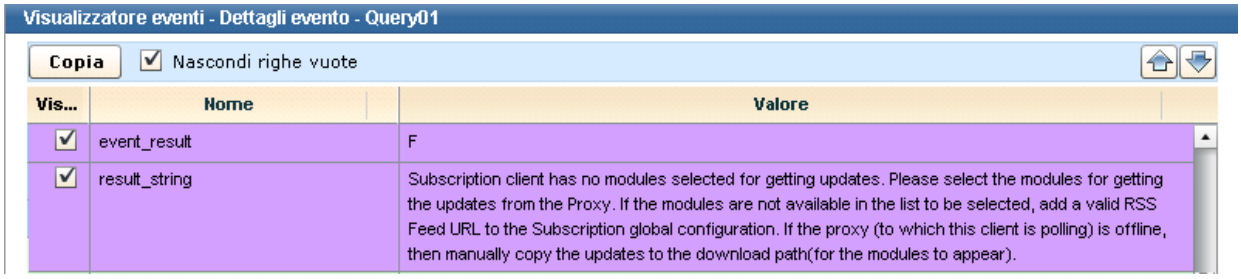
Per visualizzare i dettagli degli eventi di sottoscrizione nel visualizzatore eventi

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
2. Fare clic su Servizio di sottoscrizione in Elenco servizi.
3. Fare clic sulla scheda Eventi con monitoraggio automatico per il servizio di sottoscrizione o per un host elencato in Servizio di sottoscrizione.
4. Esaminare la colonna Descrizione risultato. Ad esempio, questa colonna può visualizzare eventi come "Nel client di sottoscrizione non sono presenti moduli selezionati per ottenere aggiornamenti".

Descrizione risultato
Subscription Client - calmrhbuildtest01 is communicating with the proxy - calmrhbuildtest01 for getting the Subscription updates.
Subscription client has no modules selected for getting updates. Please select the modules for getting the updates from the Proxy.
Unable to connect to the specified RSSFeed URL. Please check the URL again.
Unable to connect to the specified RSSFeed URL. Please check the URL again.
No modules are selected for getting updates. Please select the modules for getting the updates from the Subscription server.

5. Fare doppio clic sulla descrizione risultato per la quale si desidera visualizzare i dettagli.

   Si aprirà il visualizzatore eventi.
6. Scorrere verso il basso fino alla sezione dei risultati ed esaminare il testo visualizzato per result_string.


Visualizzatore eventi - Dettagli evento - Query01
Copia
Nascondi righe vuote
Vis...
Nome
Valore
event_result
F
result_string
Subscription client has no modules selected for getting updates. Please select the modules for getting the updates from the Proxy. If the modules are not available in the list to be selected, add a valid RSS Feed URL to the Subscription global configuration. If the proxy (to which this client is polling) is offline, then manually copy the updates to the download path(for the modules to appear).

Applicazione degli aggiornamenti di sottoscrizione agli agenti ed ai connettori

Tutti gli aggiornamenti periodici, i service pack e le versioni secondarie saranno distribuiti mediante una sottoscrizione. Spesso i moduli da scaricare comprendono gli agenti e le integrazioni. Quando questi moduli vengono scaricati in un client di sottoscrizione che gestisce gli agenti, occorre applicare tali aggiornamenti agli agenti dopo aver verificato l'avvenuto aggiornamento del client di sottoscrizione che li gestisce. Si devono applicare prima gli aggiornamenti agli agenti e poi quelli ai connettori.

Per applicare gli aggiornamenti di sottoscrizione agli agenti CA User Activity Reporting Module

1. Se l'aggiornamento comprende il modulo Agenti, aggiornare i propri agenti in base alla piattaforma, come segue:
   a. Fare clic sulla scheda Amministrazione e quindi sulla sottoscheda Raccolta registri.
   b. A seconda del livello su cui si applica ogni singola piattaforma, decidere se applicare gli aggiornamenti a tutti gli agenti contemporaneamente, ad un gruppo selezionato di essi o ad un singolo agente.
      - Se tutti gli agenti sono installati sulla stessa piattaforma, selezionare Explorer agente e fare clic su Sottoscrizione.
      - Se i gruppi di agenti sono costituiti da agenti installati sulla stessa piattaforma, espandere Explorer agente, selezionare un gruppo di agenti e fare clic su Sottoscrizione.
      - In alternativa, espandere Explorer agente e quindi un gruppo di agenti, selezionare un agente e fare clic su Sottoscrizione.

      Verrà visualizzata la procedura guidata di sottoscrizione.
   c. Se si seleziona Explorer agente o un gruppo di agenti, attivare Aggiornamenti agente, scegliere la piattaforma dall'elenco a discesa Piattaforma, fare clic su Cerca e quindi sul passaggio Selezione versione.
   d. Ser si seleziona un agente, attivare Aggiornamenti agente e fare clic sul passaggio Selezione versione.
   e. Selezionare Aggiorna versione per ogni agente elencato.
   f. Fare clic su Salva e chiudi.
   g. Verificare l'avvenuta esecuzione dell'operazione. Fare clic su Stato e comando. Fare clic sull'operazione riuscita di Configurazione. Annotare la versione della configurazione applicata.

h. Se necessario, ripetere la procedura in modo da aggiornare tutti gli agenti.

2. Se l'aggiornamento contiene il modulo Integrazioni, aggiornare i connettori per i propri agenti come segue:

   a. Fare clic sulla scheda Amministrazione e quindi sulla sottoscheda Raccolta registri.

   b. Stabilire se applicare contemporaneamente gli aggiornamenti a tutti i connettori di tutti gli agenti, ai connettori degli agenti di un gruppo selezionato, o ai connettori su un singolo agente.

   c. Selezionare Explorer agente, un gruppo di agenti o un agente. Quindi fare clic su Sottoscrizione.

   d. Dall'Elenco selezione aggiornamenti, selezionare Aggiornamenti connettore.

   e. In alternativa, per modificare il valore predefinito, Tutti, selezionare un valore da uno o più di questi elenchi a discesa: gruppo di agenti, piattaforma o integrazione. Fare clic su Cerca.

   f. Fare clic sul passaggio Selezione versione.

   g. Fare clic su Seleziona tutto per selezionare tutti i membri dell'elenco, oppure selezionare ogni riga del corrispondente connettore che si desidera aggiornare. Per ogni riga selezionata, indicare la versione dell'aggiornamento da applicare.

   h. Fare clic su Salva e chiudi.

3. Verificare gli aggiornamenti. Eseguire nuovamente la procedura guidata di sottoscrizione. Selezionare il passaggio Selezione versione per visualizzare la versione attuale e controllare che si tratti di quella selezionata per l'aggiornamento. Fare clic su Annulla.

Ulteriori informazioni:

Modalità di applicazione degli aggiornamenti di sottoscrizione (a pagina 679)
Apertura della procedura guidata Elenco aggiornamenti (a pagina 680)
Selezione degli agenti o dei connettori da aggiornare (a pagina 681)
Aggiornamento delle versioni di integrazione dell'agente o del connettore (a pagina 682)

Capitolo 8: Filtri e profili

Questa sezione contiene i seguenti argomenti:

Filtri globali e locali (a pagina 253)
Modalità di creazione di un profilo (a pagina 257)
Importazione di un profilo (a pagina 261)
Esportazione di un profilo (a pagina 262)
Impostazione di un profilo (a pagina 262)
Creazione di un filtro globale (a pagina 263)
Configurazione delle impostazioni globali delle query (a pagina 265)
Modifica di un filtro globale (a pagina 266)
Rimozione di un filtro globale (a pagina 266)
Creazione di un filtro locale (a pagina 267)
Modifica di un filtro locale (a pagina 268)
Rimozione di un filtro locale (a pagina 268)

Capitolo 9: Filtri globali e locali

È possibile impostare o modificare filtri per perfezionare le informazioni sugli eventi o gli incidenti visualizzate. Si può accedere alla finestra dei filtri globali dalla finestra principale di CA User Activity Reporting Module. È possibile aggiungere filtri locali da una singola visualizzazione di query o rapporto. È possibile utilizzare l'interfaccia dei filtri globali per impostare le opzioni delle query a livello di applicazione.

Entrambi i filtri dispongono della propria finestra di dialogo di creazione. Un unico pulsante consente di avviare ciascuna finestra di dialogo:

Filtro globale

Viene applicato a tutti i rapporti e a tutte le query visualizzati nella sessione corrente. I filtri globali *non* vengono applicati a query o rapporti ODBC esterni. Il pulsante Filtro globale viene visualizzato nella parte superiore della finestra principale di CA User Activity Reporting Module accanto al menu Server Log Manager. È possibile usare un filtro globale per visualizzare tutti gli eventi ricevuti nell'ultima settimana oppure, ad esempio, da un determinato host. È inoltre possibile applicare filtri globali per gli incidenti con la stessa metodologia utilizzata per i filtri di evento. I filtri Incidenti vengono applicati soltanto agli incidenti e alle informazioni relative agli eventi dei componenti.

Nota: per impostazione predefinita, un filtro globale restituisce informazioni sulle ultime sei ore di dati.

Filtro locale

Viene applicato soltanto alla visualizzazione corrente di rapporti, query o incidenti. Il pulsante Filtro locale viene visualizzato nella parte superiore del riquadro dei dettagli nelle visualizzazioni di query o rapporti, e nella parte superiore del riquadro Incidenti. Il filtro locale non viene applicato né salvato durante la modifica di rapporti, a meno che il rapporto venga salvato come preferito con l'impostazione di tale filtro. I filtri locali consentono di restringere una visualizzazione corrente, in modo da visualizzare, ad esempio, un solo host in una visualizzazione di rapporti relativa a più host senza cambiare le visualizzazioni degli altri rapporti.

Nota: nel caso di una query ODBC, la finestra di dialogo del filtro locale consente di impostare soltanto i filtri avanzati.

Questa sezione contiene i seguenti argomenti:

Informazioni sui filtri semplici (a pagina 254)
Impostazione di un filtro semplice (a pagina 255)
Informazioni sui filtri profilo (a pagina 256)

Informazioni sui filtri semplici

Prima di utilizzare per la prima volta la procedura guidata Progettazione query o Progettazione profilo, familiarizzare con i tipi di filtro semplice.

Esempi di filtro semplice

Segue un esempio di ogni tipo di filtro semplice:

Tipo filtro	Valore	Descrizione
Modello ideale	Antivirus	Visualizza solo i dati di evento generati da prodotti come i seguenti: ■ CA Anti-Virus ■ McAfee VirusScan ■ Symantec Antivirus Corporate Edition ■ TrendMicro OfficeScan
Categoria evento/ Classe evento	Attività di accesso/ accesso al sistema	Visualizza solo i dati evento relativi agli utenti che stanno per accedere ad un sistema.
Nome registro evento	Cisco PIX Firewall	Visualizza solo i dati evento generati dai dispositivi Cisco PIX Firewall.

Con l'eccezione di Nome registro evento, i tipi di filtro si basano sulla Grammatica evento comune (CEG, Common Event Grammar).

- Per ulteriori informazioni sui filtri basati sulla tecnologia di un prodotto, consultare l'Elenco dei modelli ideali.
- Per ulteriori informazioni sui filtri basati su una categoria, una classe o un'azione, consultare l'Elenco categorie evento e l'Elenco classi evento.

Questi elenchi si trovano nella guida in linea, nella sezione Grammatica evento comune.

Impostazione di un filtro semplice

È possibile impostare un filtro semplice per definire dei criteri per i dati evento che si desidera visualizzare o inserire in rapporti. Una volta impostati nella procedura guidata Progettazione query, i filtri semplici consentono di limitare i dati evento restituiti da una query utilizzata in un rapporto o in un avviso. Dopo l'impostazione nella procedura guidata Progettazione query, i filtri semplici limitano i dati visualizzati nei risultati di rapporto o di query quando viene applicato il profilo.

1. Aprire la procedura guidata.
2. Definire il tipo di filtro semplice da impostare:
   - basato su una tecnologia;
   - basato su una categoria, su una categoria e su una classe, oppure su una categoria, una classe ed un'azione;
   - basato su un prodotto.
3. Per impostare un filtro basato su una tecnologia, fare clic sulla casella di controllo Il modello ideale è, e selezionare un valore dall'elenco a discesa Modello ideale.
4. Per impostare un filtro basato su una categoria, una categoria e una classe, una categoria, una classe ed un'azione di evento di protezione, eseguire le seguenti operazioni:
   a. Fare clic sulla casella di controllo Categoria evento e selezionare un valore dall'elenco a discesa associato.
   b. (Facoltativo). Fare clic sulla casella di controllo Classe evento e selezionare un valore dall'elenco discesa associato.
   c. (Facoltativo). Se è stato selezionato Classe evento, fare clic sulla casella di controllo Azione evento, e quindi selezionare un valore dall'elenco a discesa.

   Nota: è possibile anche impostare questo filtro di tipo sotto un filtro basato su una tecnologia.
5. Per impostare un filtro basato su un prodotto, fare clic sulla casella di controllo Il nome di registro evento è, e selezionare un valore dall'elenco a discesa.
6. Completare la procedura guidata.

Informazioni sui filtri profilo

Un profilo è un gruppo di filtri. È possibile creare un profilo con filtri tag, filtri dati o con una combinazione di essi. Il filtro tag query limita le query visualizzate per la selezione corrente. Il filtro tag di rapporto limita i rapporti visualizzati per la selezione. I filtri dati limitano i dati visualizzati nei risultati di un rapporto o di una query. I filtri di profilo si applicano a query, rapporti e ad avvisi e rapporti pianificati.

È possibile scegliere separatamente i filtri tag per i rapporti e per le query. Seguono alcuni esempi di filtri tag:

- I tag basati su standard come COBIT, FISMA, GLBA, HIPAA, NERC, PCI, SAS 70, SOX.

  I filtri tag basati su uno standard relativi ai tag di rapporto e non ai tag di query.
- I tag di categoria evento di protezione, come protezione del contenuto, protezione dell'host, protezione di rete, protezione operativa, accesso alle risorse e accesso al sistema.
- I tag di prodotto, come CA Access Control, CA Identity Manager e CA SiteMinder.

È possibile selezionare un filtro dati semplice oppure crearne uno avanzato. Segue una descrizione di ognuno di essi:

- I filtri dati semplici possono basarsi su uno qualsiasi degli elementi seguenti:
  - Una tecnologia selezionata (software di sistema, software applicativo di host e servizi, software applicativo e servizi di rete).
  - Una categoria, una categoria e una classe oppure una categoria, una classe ed un'azione selezionate di evento CEG.
  - Un prodotto selezionato.
- I filtri dati avanzati si basano su query SQL definite dall'utente composte da una o più clausole WHERE. La query seleziona una colonna CEG con una clausola WHERE composta da tale colonna CEG, da un operatore e da un valore selezionati.

Modalità di creazione di un profilo

È possibile creare profili in modo tale da consentire agli utenti di restringere le visualizzazioni di CA User Activity Reporting Module in base alle esigenze del proprio ambiente. Ad esempio, è possibile creare un profilo di CA Access Control che consente di visualizzare solo i rapporti, le query e gli eventi relativi ad Access Control.

Il procedimento di creazione di un profilo con procedura guidata si basa sui seguenti passaggi:

1. Apertura dell'impostazione guidata profilo
2. Assegnazione di un nome al profilo ed inserimento di informazioni descrittive
3. Identificazione delle informazioni visualizzate tramite filtri semplici ed avanzati
4. Selezione di query e rapporti da visualizzare utilizzando filtri tag.

Ulteriori informazioni:

Aggiunta di dettagli al profilo (a pagina 258)
Creazione dei Filtri dati (a pagina 259)
Creazione di Filtri tag (a pagina 260)

Aprire l'impostazione guidata profilo

Per creare un nuovo profilo o per modificarne uno esistente, aprire l'impostazione guidata profilo.

Per aprire l'impostazione guidata profilo

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria.

   Viene visualizzato l'elenco della cartella Libreria.

2. Selezionare la cartella Profili.

   Nel riquadro dei dettagli verrà visualizzato il pulsante Profili.

3. Fare clic su Nuovo profilo:

   Verrà visualizzata l'impostazione guidata profili.

   Quando si utilizza la procedura guidata:

   - Fare clic su Salva per salvare il file della regola senza chiudere la procedura guidata.
   - Fare clic su Salva e chiudi per salvare il file della regola e chiudere la procedura guidata.
   - Fare clic su Reimposta per ripristinare la visualizzazione della procedura guidata alle ultime impostazioni salvate.

Aggiunta di dettagli al profilo

È necessario assegnare un nome ai profili. È anche possibile immettere informazioni descrittive facoltative da usare come riferimento.

Per assegnare un nome ad un profilo

1. Aprire l'impostazione guidata profilo.
2. Immettere un nome per il nuovo profilo. Il nome può essere lungo fino a 80 caratteri e può comprendere anche caratteri speciali.
3. (Facoltativo) Digitare delle informazioni descrittive.
4. Avanzare fino al passaggio Filtri dati.

Creazione dei Filtri dati

È possibile filtrare le informazioni visualizzate nel proprio profilo tramite filtri semplici o avanzati. Ogni profilo deve disporre almeno di un filtro.

Per impostare i filtri dati di un profilo

1. Aprire l'impostazione guidata profilo.
2. Inserire il nome del profilo, se non già specificato, e procedere fino al passaggio Filtri dati.

   Verrà visualizzata la finestra di dialogo relativa ai filtri, contenente la scheda Filtri semplici.
3. Creare i filtri semplici desiderati. Ad esempio, è possibile selezionare la casella Nome registro evento, ed inserire "CA Access Control" per cercare gli eventi di CA Access Control.
4. (Facoltativo) Fare clic sulla scheda Filtri avanzati.

   Verrà visualizzata la finestra di dialogo Filtri avanzati.
5. Creare i filtri avanzati in base alle proprie esigenze.
6. Fare clic sulla freccia appropriata per andare al passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Facendo clic su Salva e chiudi, nell'elenco verrà visualizzato il nuovo profilo. In alternativa, apparirà il passaggio scelto della procedura guidata.

Ulteriori informazioni

Creazione di un filtro evento semplice (a pagina 584)
Creazione di un filtro di eventi avanzato (a pagina 586)
Utilizzo di filtri avanzati (a pagina 584)

Creazione di Filtri tag

È possibile creare filtri per tag da applicare al proprio profilo, in modo da controllare i tag relativi a query o categorie di rapporti che verranno visualizzati nell'interfaccia di CA User Activity Reporting Module una volta applicato il profilo utente. Ad esempio, se si crea un filtro per il tag <stmdnr>, nell'interfaccia di CA User Activity Reporting Module verranno visualizzati solo i rapporti e le query che presentano il tag CA SiteMinder.

Per creare un filtro tag

1. Aprire l'impostazione guidata profilo.
2. Inserire il nome del profilo, se non già specificato, e proseguire fino al passaggio Filtri tag.

   Verrà visualizzata la finestra di dialogo relativa ai filtri, con all'interno la sottoscheda Filtri tag di rapporto.
3. Fare clic su Nuovo filtro evento.

   La prima riga della tabella del filtro tag diventerà attiva.
4. Fare clic sulla cella Tag e selezionare o digitare il nome del tag della query o del rapporto da visualizzare. Durante la digitazione, si ridurranno i nomi dei tag disponibili.
5. (Facoltativo) Per aggiungere altri filtri, fare clic una seconda volta su Nuovo filtro evento.

   La seconda riga della tabella dei filtri tag diventerà attiva, visualizzando AND nella colonna degli operatori logici.
6. (Facoltativo) Fare clic sulla cella degli operatori logici e selezionare AND o OR.
7. (Facoltativo) Fare clic sulla cella Tag e selezionare o digitare il nome del tag da visualizzare. Durante la digitazione, si ridurranno i nomi dei tag disponibili.
8. (Facoltativo) Fare doppio clic sulle celle relative alle parentesi aperte e chiuse ed immettere il numero di parentesi necessarie.
9. (Facoltativo) Fare clic sulla sottoscheda Filtri tag query e ripetere i passaggi dal 3 all'8 per creare i filtri tag query necessari.
10. Una volta immesse le istruzioni dei filtri desiderate, fare clic su Salva.

Ulteriori informazioni:

Creazione dei Filtri dati (a pagina 259)

Importazione di un profilo

È possibile importare un profilo, operazione che consente di spostare i profili da un ambiente all'altro. Ad esempio, si può importare nel proprio ambiente dinamico un profilo creato in un ambiente di prova.

Per importare un profilo

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria.

   Viene visualizzato l'elenco della cartella Libreria.

2. Per espandere la cartella Profili, fare clic sulla freccia accanto ad essa.

   Nel riquadro dei dettagli verrà visualizzato il pulsante Profili.

3. Fare clic su Importa profilo.

   Verrà visualizzata la finestra di dialogo Importa file.

4. Individuare il file da importare e fare clic su OK.

   Verrà visualizzata l'impostazione guidata profilo, contenente i dettagli del profilo selezionato.

5. Apportare le modifiche desiderate e fare clic su Salva e chiudi. Se il profilo importato ha lo stesso nome di un altro già presente nel proprio database di gestione, verrà richiesto di modificarne il nome.

   Il profilo importato verrà visualizzato nella cartella corretta.

Esportazione di un profilo

È possibile esportare un profilo. Ciò consente di condividere i profili fra diversi ambienti. Ad esempio, è possibile esportare nel proprio ambiente dinamico un un profilo creato in un ambiente di prova.

Per esportare un profilo

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria.

   Viene visualizzato l'elenco della cartella Libreria.

2. Per espandere la cartella Profili, fare clic sulla freccia accanto ad essa.

   Verranno visualizzate le cartelle dei profili.

3. Fare clic sulla cartella che contiene il profilo da esportare.

   La cartella si espanderà, mostrando i singoli file in essa contenuti.

4. Selezionare il profilo da esportare e fare clic su Esporta profilo.

   Verrà visualizzata la finestra di dialogo relativa alla posizione dell'esportazione.

5. Inserire o andare fino alla posizione in cui memorizzare il profilo esportato, e fare clic su Salva.

   Verrà visualizzata una finestra di conferma dell'avvenuta esportazione.

6. Fare clic su OK.

   Il profilo è stato esportato.

Impostazione di un profilo

È possibile selezionare qualsiasi profilo disponibile per applicarlo al proprio ambiente, limitando le query ed i rapporti disponibili a seconda dei termini del profilo. Per impostare un profilo, selezionarne uno dal menu a discesa Profili, che si trova nella parte superiore della finestra principale di CA User Activity Reporting Module.

Nota:per impostare il profilo selezionato come profilo predefinito del proprio ambiente, fare clic su Imposta come profilo predefinito, nella parte superiore dalla pagina principale di CA User Activity Reporting Module Il profilo selezionato viene impostato come profilo predefinito dell'utente connesso.

Creazione di un filtro globale

È possibile creare un filtro globale. I filtri globali consentono di visualizzare tutte le query e i rapporti, oppure tutti gli incidenti, utilizzando gli stessi fattori di qualificazione. Quando si crea un filtro globale, è possibile scegliere se si applica agli eventi o agli incidenti. Non è possibile applicare un unico filtro globale ad entrambi. È possibile utilizzare l'interfaccia dei filtri globali per impostare le opzioni delle query a livello di applicazione.

Per creare un filtro globale

1. Fare clic sul pulsante Filtri globali nella parte superiore della finestra principale.

   Verrà visualizzata la finestra di dialogo Filtri e impostazioni globali.

2. Fare clic sulla scheda Eventi o sulla scheda Incidenti per indicare dove si desidera applicare il filtro globale.

3. Specificare il periodo di tempo in cui applicare il filtro alla ricerca mediante l'elenco a discesa Intervallo di tempo.

4. Selezionare la casella di controllo Corrispondenza per immettere un valore specifico in base al quale filtrare tutti gli eventi non elaborati disponibili.

   Nota: è possibile ricercare più valori, frasi o valori parziali negli eventi non elaborati mediante la sintassi di corrispondenza specifica.

5. Fare clic su Aggiungi filtro per specificare i campi di evento da includere nel filtro.

   Vengono visualizzati il menu a discesa Colonna e il campo di immissione Valore.

6. Scegliere il campo di evento da includere nel filtro, quindi digitare il valore del campo da visualizzare nei rapporti filtrati. Selezionare di nuovo Aggiungi filtro per immettere ulteriori nomi e valori di campi di evento. Selezionare il pulsante Escludi per includere *soltanto* il valore immesso per il nome del campo di evento selezionato.

   Nota: se si crea un filtro globale per un campo di tipo stringa, il filtro verrà aggiunto all'elenco dei filtri rapidi. Se si crea un filtro per un campo numerico o che riporta l'ora, il filtro verrà aggiunto all'elenco dei filtri avanzati.

7. (Facoltativo) Fare clic sulla scheda Filtri avanzati per aggiungere ulteriori qualificatori complessi.

8. (Facoltativo) Fare clic sulla scheda Impostazioni per scegliere le impostazioni globali. Queste impostazioni vengono applicate all'intera applicazione.

9. (Facoltativo) Selezionare Imposta come predefinito nella parte inferiore della finestra di dialogo per mantenere le impostazioni del filtro nelle sessioni successive fino a quando si rimane connessi.
10. Fare clic su Salva.

    La finestra di dialogo Filtri globali e Impostazioni viene chiusa e il nuovo filtro viene applicato ai rapporti.

Ulteriori informazioni:

Utilizzo di filtri avanzati (a pagina 584)

Configurazione delle impostazioni globali delle query

Tramite la finestra di dialogo Filtri globali, è possibile impostare condizioni a livello dell'applicazione che si applichino a tutti i rapporti e le query nel proprio ambiente. Le impostazioni globali vengono applicate a tutta la sessione corrente, a meno che vengano impostate come valori predefiniti.

Per configurare le impostazioni globali delle query

1. Fare clic sul pulsante Filtri globali nella parte superiore della finestra principale.

   Viene visualizzata la finestra di dialogo Filtri globali e Impostazioni, in cui è disponibile la scheda Filtri rapidi.

2. Fare clic sulla scheda Impostazioni.

   Viene aperta la scheda, che mostra i valori seguenti.

   Fuso orario locale

   Controlla il fuso orario di tutti i campi data/ora di rapporti e query. I rapporti e le query adottano il fuso orario selezionato dall'elenco a discesa piuttosto che utilizzare quello del server CA User Activity Reporting Module.

   Esegui query sui dati federati

   Consente l'applicazione delle query a tutti i server federati disponibili. Questa funzione è attivata per impostazione predefinita. La disattivazione dell'impostazione limita le query ai soli dati evento memorizzati nel deposito eventi di log. Consente di aumentare la velocità di query se gli eventi di destinazione sono archiviati in locale.

   Nota: l'impostazione dei dati federati non viene applicata alle query esterne ODBC.

   Attiva aggiornamento automatico per le query

   Consente l'aggiornamento automatico della visualizzazione agli intervalli impostati per ogni query.

3. (Facoltativo) Selezionare Imposta come predefinito nella parte inferiore della finestra di dialogo per mantenere le impostazioni come elementi predefiniti che verranno memorizzati al termine della sessione corrente.

4. Apportare le modifiche desiderate, quindi fare clic su Salva.

   La finestra di dialogo Filtri e impostazioni globali viene chiusa e viene applicato il nuovo filtro.

Modifica di un filtro globale

È possibile modificare un filtro globale esistente.

Per modificare un filtro globale

1. Fare clic sul pulsante Filtri globali nella parte superiore della finestra principale.

   Viene visualizzata la finestra di dialogo Filtri globali e Impostazioni, in cui è disponibile la scheda Filtri rapidi.

2. Modificare o aggiungere parametri secondo necessità. Fare clic sull'icona Elimina accanto al parametro di un singolo filtro rapido per rimuoverlo.

3. Fare clic su Salva.

   Le finestre di dialogo Filtri globali e Impostazioni vengono chiuse e il filtro modificato viene applicato.

Rimozione di un filtro globale

È possibile rimuovere un filtro globale, riportando tutti i rapporti allo stato predefinito.

Per rimuovere un filtro globale, fare clic su Elimina filtri globali nella parte superiore della finestra principale di CA User Activity Reporting Module:

Creazione di un filtro locale

È possibile creare un filtro locale per restringere l'ambito della query o del rapporto visualizzato, o gli incidenti visualizzati nell'area Incidenti.

Per creare un filtro locale

1. Aprire il rapporto o la query che si desidera filtrare, oppure fare clic sulla scheda Incidenti, quindi fare clic sul pulsante Filtri locali nella parte superiore del riquadro.

   Verrà visualizzata la finestra di dialogo Filtri locali, in cui è disponibile la scheda Filtri rapidi.

2. (Facoltativo) Fare clic sulla scheda Incidenti per filtrare gli incidenti visualizzati anziché gli eventi.

3. (Facoltativo) Selezionare la casella di controllo Corrispondenza per digitare un valore specifico in base al quale ricercare eventi o incidenti.

   Nota: è possibile ricercare più valori, frasi o valori parziali mediante la sintassi di corrispondenza specifica.

4. Fare clic su Aggiungi filtro.

5. Scegliere il campo di evento da includere nel filtro, quindi digitare il valore del campo da visualizzare nei rapporti filtrati. Selezionare di nuovo Aggiungi filtro per immettere più valori di colonne. Selezionare il pulsante Escludi per includere *soltanto* il valore immesso per il nome del campo di evento selezionato.

6. (Facoltativo) Fare clic sulla scheda Filtri avanzati per aggiungere ulteriori indicatori.

7. Fare clic su Salva.

   Il filtro viene applicato alla visualizzazione. È possibile salvare la visualizzazione del rapporto impostandola come preferito.

Modifica di un filtro locale

È possibile modificare un filtro locale esistente.

Per modificare un filtro locale

1. Fare clic sul pulsante Filtri locali nella parte superiore del riquadro della query o del rapporto, oppure nella parte superiore del riquadro Incidenti.

   Verrà visualizzata la finestra di dialogo Filtri locali, in cui è disponibile la scheda Filtri rapidi.

2. Modificare o aggiungere valori secondo necessità. Per rimuovere impostazioni di filtri singoli, fare clic sull'icona Elimina accanto a ciascun filtro. Per rimuovere un valore Corrispondenza, deselezionare la relativa casella di controllo.

3. Fare clic su Salva.

   Il filtro modificato viene applicato alla visualizzazione.

Rimozione di un filtro locale

È possibile rimuovere un filtro locale, riportando una visualizzazione di query, rapporto o incidente allo stato precedente.

Per rimuovere un filtro locale, fare clic sul pulsante Elimina filtro locale nella parte superiore della visualizzazione di query, rapporto o incidente corrente:

Capitolo 10: Query e rapporti

Questa sezione contiene i seguenti argomenti:

Informazioni su query e rapporti (a pagina 270)
Attività relative ai tag (a pagina 273)
Formato data/ora (a pagina 274)
Visualizzazione di una query (a pagina 278)
Visualizzazione di un rapporto (a pagina 279)
Disattivazione dell'opzione Mostra rapporto selezionato (a pagina 281)
Esempio: esecuzione di rapporti PCI (a pagina 282)
I prompt (a pagina 287)
Come creare una query (a pagina 305)
Modifica di una query (a pagina 325)
Eliminazione di una query personalizzata (a pagina 325)
Disattivazione dell'opzione Mostra query selezionata (a pagina 326)
Esportazione e importazione delle definizioni delle query (a pagina 326)
Modalità di creazione di un rapporto (a pagina 329)
Esempio: creazione di un rapporto da query esistenti (a pagina 333)
Esempio: impostazione della federazione e dei rapporti federati (a pagina 337)
Modifica di un rapporto (a pagina 342)
Eliminazione di un rapporto personalizzato (a pagina 342)
Esportazione delle definizioni dei rapporti (a pagina 345)
Importazione delle definizioni dei rapporti (a pagina 346)
Preparazione all'utilizzo di rapporti dotati di elenchi con chiave (a pagina 347)
Visualizzare un rapporto utilizzando un elenco con chiave (a pagina 364)

Informazioni su query e rapporti

È possibile utilizzare le query nei seguenti modi:

- È possibile eseguire una query per visualizzare i dati di un evento o incidente quasi in tempo reale.
- È possibile selezionare un rapporto predefinito per visualizzare i risultati di più query correlate.
- È possibile creare un rapporto composto di query selezionate dall'utente.
- È possibile utilizzare le query con richiesta di conferma per ricercare specifiche informazioni preselezionate.
- È possibile pianificare l'esecuzione di query su dati recenti come avvisi per l'invio di notifiche via posta elettronica alle parti responsabili. Gli avvisi vengono aggiunti anche a un feed RSS che può essere visualizzato mediante lettori di terze parti.
- È possibile creare query personalizzate per la visualizzazione o la creazione di avvisi o rapporti.

Esistono due tipi di query e rapporti:

- Le query e i rapporti di *sottoscrizione* sono predefiniti da CA e vengono forniti insieme all'applicazione CA User Activity Reporting Module al momento dell'installazione oppure aggiunti con un aggiornamento di sottoscrizione.
- Le query e i rapporti *utente* sono quelli creati da un utente. È possibile creare una query o un rapporto da zero oppure crearne uno a partire da una query o un rapporto di sottoscrizione che si desidera modificare.

CA User Activity Reporting Module fornisce un elenco completo delle query e dei rapporti di sottoscrizione. Se all'utente è stato assegnato il ruolo di revisore, analista o amministratore, è in grado di visualizzare tutte le query e i rapporti di sottoscrizione. Inoltre, su una query o un rapporto di sottoscrizione correntemente visualizzati è possibile eseguire le seguenti azioni:

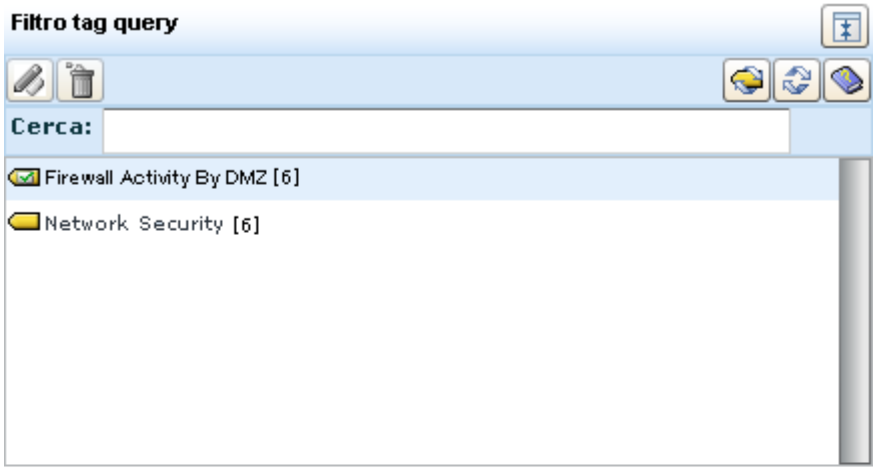
- Aggiornare i dati visualizzati.
- Modificare i filtri locali per nascondere i dati che non si desidera visualizzare.
- Eliminare i filtri locali per visualizzare di nuovo le query o rapporti senza filtri.
- Aggiungere query o rapporti visualizzati all'elenco dei preferiti.
- Stampare la query.
- Modificare l'opzione che mostra la query o il rapporto selezionati.
- Chiudere la query o il rapporto visualizzati.

Solo gli utenti cui è stato assegnato il ruolo di analista o amministratore possono eseguire le seguenti azioni:

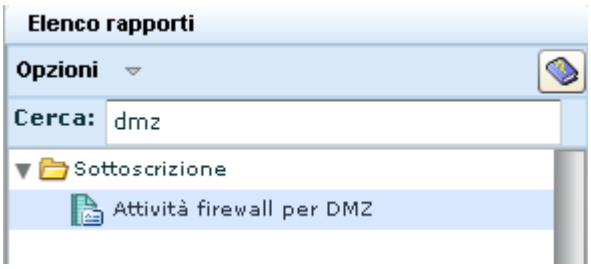
- Creare una query o un rapporto utente completamente nuovi.
- Copiare una query o un rapporto di sottoscrizione e utilizzarlo come base per una query o un rapporto utente.
- Modificare una query o un rapporto utente.
- Esportare una query o un rapporto utente.
- Eliminare una query o un rapporto utente.
- Salvare le modifiche alla query o al rapporto utente selezionati.
- Importare la definizione di una query o di un rapporto utente.

Esempio delle query e dei rapporti corrispondenti

Prendere in considerazione il tag query Attività firewall di DMZ. Notare che è associato a sei query separate in questo argomento.



Le query visualizzate nell'elenco delle query vengono utilizzate nei rapporti. Dalla scheda Rapporti è possibile visualizzare un rapporto chiamato Attività firewall di DMZ.



Nell'illustrazione seguente sono mostrati soltanto i nomi. Notare che ogni nome rispecchia una delle sei query del rapporto. La maggior parte dei rapporti include i risultati delle query per riepilogo, tendenza e dettaglio.

Attività relative ai tag

I tag consentono di associare rapporti e query a categorie per facilitare i riferimenti e di fornire un framework organizzativo per la creazione di rapporti sull'ambiente di lavoro. I tag di categoria permettono inoltre di suddividere facilmente il carico di lavoro in base al ruolo o al tipo di evento.

È possibile utilizzare i tag predefiniti oppure creare tag personalizzati per i rapporti e le query. Ad esempio, è possibile creare un tag Mensile da aggiungere ai rapporti da pianificare mensilmente per semplificare i riferimenti e la visualizzazione. In questo modo, è inoltre possibile aggiungere o rimuovere rapporti dai processi di rapporto senza modificare i processi stessi: è sufficiente, infatti, aggiungere il tag Mensile a un nuovo processo o rimuoverlo da uno precedente.

Si possono aggiungere tag personalizzati per query o rapporti individuali come parte del processo di creazione di rapporti o di modifica. Una volta creato un nuovo tag, il relativo titolo viene visualizzato nell'elenco dei tag; a questo punto è possibile selezionarlo per aggiungerlo ad altri report o query.

I tag personalizzati possono essere rinominati o eliminati. È possibile rimuovere i tag personalizzati dai rapporti o query che li includono modificando il rapporto o la query.

Capitolo 11: Formato data/ora

CA User Activity Reporting Module utilizza file di proprietà delle impostazioni locali diversi per visualizzare il contenuto localizzato dell'interfaccia utente. CA User Activity Reporting Module fornisce i seguenti file di impostazioni locali nella directory /opt/CA/LogManager/locale:

- de_ui.properties
- en_ui.properties
- fr_ui.properties
- ja_ui.properties
- es_ui.properties
- it_ui.properties

L'aggiornamento dei file di proprietà delle impostazioni locali viene eseguito mediante la pubblicazione di nuove versioni, service pack e sottoscrizioni. È possibile utilizzare questi file di proprietà delle impostazioni locali per modificare il formato predefinito della data e dell'ora nel formato desiderato. Il formato data/ora configurato viene visualizzato nell'interfaccia utente e nei risultati di query e rapporti.

Questa sezione contiene i seguenti argomenti:

Formati data/ora supportati (a pagina 275)
Modifica del formato data/ora (a pagina 277)

Formati data/ora supportati

CA User Activity Reporting Module supporta i seguenti formati data/ora:

Lettera di riferimento	Descrizione
Y	Indica l'anno. I valori disponibili sono: ■ Due lettere ■ Quattro lettere Se il valore è definito su due lettere, viene sostituito da due cifre. Ad esempio, YY=11 per l'anno 2011. Se il valore è definito su quattro lettere, viene sostituito dal testo completo. Ad esempio, YYYY=2011.
M	Indica un mese. I valori disponibili sono: ■ Una lettera ■ Due lettere ■ Tre lettere ■ Quattro lettere Se il valore è definito su una lettera, viene sostituito da una o due cifre. Ad esempio, M=1 o 11. Se il valore è definito su due lettere, viene sostituito da due cifre. Ad esempio, MM=01. Se il valore è definito su tre lettere, viene sostituito da tre lettere. Ad esempio, MMM=gen. Se il valore è definito su quattro lettere, viene sostituito dal testo completo. Ad esempio, MMMM=gennaio.
D	Indica un giorno del mese. I valori disponibili sono: ■ Una lettera ■ Due lettere Se il valore è definito su una lettera, viene sostituito da una o due cifre. Ad esempio, D=1 o 11. Se il valore è definito su due lettere, viene sostituito da due cifre. Ad esempio, DD=01 o 11.

Lettera di riferimento	Descrizione
E	Indica un giorno della settimana. I valori disponibili sono: ■ Tre lettere ■ Quattro lettere Se il valore è definito su tre lettere, viene sostituito da tre lettere. Ad esempio, EEE=lun. Se il valore è definito su quattro lettere, viene sostituito dal testo completo. Ad esempio, EEEE=lunedì.
A	Indica un formato di ora. I valori disponibili sono: ■ AM ■ PM
J	Indica l'ora in formato 24 ore (0-23).
H	Indica l'ora in formato 24 ore (1-24).
K	Indica l'ora in formato 12 ore (0-11).
L	Indica l'ora in formato 12 ore (1-12).
N	Indica il minuto. I valori disponibili sono: ■ Una lettera ■ Due lettere Se il valore è definito su una lettera, viene sostituito da una o due cifre. Ad esempio, N=1 o 11. Se il valore è definito su due lettere, viene sostituito da due cifre. Ad esempio, NN=01 o 11.
S	Indica il secondo. Il valore disponibile è: ■ Due lettere Se il valore è definito su due lettere, viene sostituito da due cifre. Ad esempio, SS=01 o 11.
Q	Specifica il millisecondo. I valori disponibili sono: ■ Due lettere ■ Tre lettere Se il valore è definito su due lettere, viene sostituito da due cifre. Ad esempio, QQ=01 o 11. Se il valore è definito su tre lettere, viene sostituito da tre cifre. Ad esempio, QQQ=001.

Ad esempio, se la data corrente è 11 febbraio 2011 e l'ora corrente è 14.20 e 12 secondi sull'orologio in formato 24 ore, il valore data/ora può essere rappresentato con uno dei seguenti formati:

- EEEE, MMM. D, YYYY J:NN:QQQ—venerdì, feb. 11, 2011 14:20:012
- EEEE, MMM. D, YYYY K:NN:SS A—venerdì, feb. 11, 2011 2:20:12 PM
- DD/MM/YYYY—11/02/2011
- MM/DD/YYYY—02/11/2011

Modifica del formato data/ora

Per modificare il formato data/ora, eseguire i seguenti passaggi:

1. Creare un file di proprietà delle impostazioni locali. Ad esempio, se la lingua del browser in uso è l'inglese e si desidera utilizzare il formato data/ora della Gran Bretagna, creare un file di proprietà delle impostazioni locali denominato en-GB_ui.properties.

   Nota: il nome del file di proprietà delle impostazioni locali deve corrispondere al nome lingua visualizzato nelle impostazioni lingua del browser.
2. Copiare il contenuto del file en_ui.properties nel file delle impostazioni locali en-GB_ui.properties.
3. Aprire il file en-GB_ui.properties e modificare le proprietà dateFormat e formatString.
4. Salvare le modifiche.
5. Riavviare iGateway.

Nota: è necessario aggiornare il file di proprietà delle impostazioni locali creato con il contenuto più recente del file di proprietà delle impostazioni locali di CA User Activity Reporting Module. Una volta eseguito l'aggiornamento, è possibile personalizzare tale file.

Ulteriori informazioni:

Formati data/ora supportati (a pagina 275)

Visualizzazione di una query

Tutti gli utenti cui è stato assegnato il ruolo di revisore, analista o amministratore possono visualizzare tutte le query. Le query predefinite sono elencate nella cartella Sottoscrizione. Dopo aver definito la prima query personalizzata, viene aggiunta una cartella Utente all'elenco query per registrare la query personalizzata. Dopodichè, tutte le query personalizzate vengono aggiunte alla cartella Utente.

Per visualizzare una query

1. Fare clic sulla scheda Query e rapporti, quindi selezionare la sottoscheda Query.

   Nel riquadro di sinistra vengono visualizzati il pulsante di ingrandimento Filtro tag query, l'Elenco query, il menu Opzioni e la casella di testo Cerca.

2. Selezionare la query da visualizzare in uno dei modi seguenti:

   - Scorrere l'elenco delle query e selezionare la query che si desidera visualizzare.
   - Immettere una parola chiave nella casella Cerca per visualizzare solo le query il cui nome contiene la parola specificata.
   - Selezionare un tag visualizzato o inserire una parola chiave nella casella Cerca per limitare il numero dei tag visualizzati. Selezionare un tag per visualizzare le query correlate. Selezionare la query che si desidera visualizzare.
   - Se si desidera individuare una query personalizzata, minimizzare la cartella Sottoscrizione ed espandere la cartella Utente, quindi scorrere l'elenco della cartella Utente.

   La query selezionata viene visualizzata nel riquadro dei dettagli in formato tabella. I risultati più recenti vengono visualizzati per primi nella tabella dei risultati. Per visualizzare altri risultati, fare clic sui tasti di direzione oppure selezionare un intervallo di righe dall'elenco.

   Nota: se i risultati della query non vengono raggruppati, l'elenco mostra l'intervallo di righe visualizzato e l'intervallo sequenziale successivo disponibile. Se i risultati della query vengono raggruppati, l'elenco mostra tutti gli intervalli di righe disponibili nell'intero set di risultati.

3. (Facoltativo) Eseguire una delle operazioni seguenti:
   - Impostare i filtri facendo clic su Modifica filtri locali, per visualizzare solo i dati desiderati. Per ripristinare la visualizzazione originale della query, fare clic su Cancella filtri locali.
   - Fare clic su Aggiungi a Preferiti per aggiungere la query o il rapporto visualizzati al proprio elenco dei preferiti.
   - Fare clic su Aggiorna per aggiornare i dati con le aggiunte più recenti.
   - Fare clic su Stampa per stampare la query.
4. Fare clic su Chiudi per chiudere la query visualizzata.

Visualizzazione di un rapporto

Tutti gli utenti cui è stato assegnato il ruolo di revisore, analista o amministratore possono visualizzare tutti i rapporti. I rapporti predefiniti sono elencati nella cartella Sottoscrizione. Una volta definito il primo rapporto personalizzato, all'elenco dei rapporti viene aggiunta una cartella Utente contenente il rapporto personalizzato. Dopodichè, tutti i rapporti personalizzati vengono aggiunti alla cartella Utente.

La selezione di un rapporto dall'elenco relativo comporta l'esecuzione delle query che costituiscono il rapporto sui record di registro attualmente presenti negli archivi registro utente interni. I risultati del rapporto, visualizzati nel riquadro di sinistra, provengono dagli archivi registro eventi del server CA User Activity Reporting Module attivo e dei server figli.

Per visualizzare un rapporto, procedere come segue.

1. Fare clic sulla scheda Query e rapporti, quindi sulla sottoscheda Rapporti.

   Nel riquadro di sinistra vengono visualizzati il pulsante di ingrandimento Filtro tag di rapporto, l'Elenco rapporti e il menu Opzioni.

2. Dal menu Opzioni, scegliere Mostra rapporto selezionato, in caso la selezione non sia già stata operata.

   Questo consente di visualizzare tutti gli eventuali rapporti selezionati nel riquadro destro.

3. Selezionare il rapporto da visualizzare in uno dei modi seguenti:

   - Scorrere l'elenco dei rapporti e selezionarne uno da visualizzare.
   - Inserire una parola chiave nel campo di immissione Cerca e selezionare un rapporto da visualizzare dall'elenco filtrato.
   - Fare clic sul pulsante di ingrandimento per visualizzare l'elenco dei filtri tag di rapporto. Selezionare un tag visualizzato o inserire una parola chiave nella casella Cerca per limitare il numero dei tag visualizzati. Selezionare un tag per visualizzare i relativi rapporti. Selezionare un rapporto da visualizzare.
   - Se si sta cercando un rapporto personalizzato, comprimere la cartella Sottoscrizione, espandere la cartella Utente e scorrere tutto l'elenco della cartella Utente.

   Il rapporto selezionato viene visualizzato nel riquadro principale della pagina.

4. (Facoltativo) Eseguire una qualsiasi delle seguenti azioni:

   - Fare clic su Modifica filtri locali per visualizzare soltanto i dati che si desidera visualizzare. Per ripristinare la visualizzazione originale del rapporto, fare clic su Elimina filtri locali.
   - Fare clic su Aggiungi a Preferiti per aggiungere il rapporto visualizzato al proprio elenco dei preferiti.
   - Fare clic su Aggiorna per aggiornare i dati con le aggiunte più recenti.
   - Fare clic su Stampa per stampare il rapporto.

5. Fare clic su Chiudi per chiudere il rapporto visualizzato.

Disattivazione dell'opzione Mostra rapporto selezionato

È possibile impostare il proprio elenco rapporti in modo da poter apportare grandi modifiche senza caricare i rapporti. Generalmente, la selezione di un rapporto dall'elenco ne apre la visualizzazione nella finestra dei dettagli.

La disattivazione di questa modalità predefinita consente di risparmiare tempo e di selezionare un rapporto dall'elenco e modificarlo immediatamente, senza doverne attendere la visualizzazione. Ciò risulta utile in particolare se si devono modificare parecchi rapporti e si conoscono già le modifiche da apportare.

Dato che soltanto gli utenti con modalità amministratore o analista possono creare o modificare i rapporti, essi saranno i soli che potranno disattivare l'impostazione Mostra rapporto selezionato.

Per disattivare l'opzione Mostra rapporto selezionato

1. Fare clic su Opzioni nella parte superiore dell'Elenco rapporti.

   Viene visualizzato il menu Opzioni.

2. Deselezionare la casella di controllo accanto a Mostra rapporto selezionato.

   Nessun rapporto selezionato dall'elenco verrà visualizzato fino a quando questa opzione non verrà nuovamente abilitata.

Ulteriori informazioni

Modalità di creazione di un rapporto (a pagina 329)
Modifica di un rapporto (a pagina 342)

Esempio: esecuzione di rapporti PCI

Il PCI Security Standards Council è un forum globale aperto responsabile della distribuzione del PCI Data Security Standard (PCI DSS) che definisce i requisiti per la gestione della protezione, per i criteri e per le procedure. Le organizzazioni che archiviano, elaborano o trasmettono dati dei titolari di carta di credito devono essere conformi allo standard PCI DSS versione 1.2, che elenca in dettaglio dodici requisiti.

CA User Activity Reporting Module fornisce rapporti PCI out-of-the-box che possono essere visualizzati non appena il proprio sistema inizia a raccogliere ed elaborare i registri eventi.

Gli esempi in questa sezione aiutano a familiarizzare con i rapporti PCI e con la loro pianificazione e distribuzione. Gli esempi includono riferimenti al numero associato al requisito PCI DDS cui si riferisce il rapporto.

Ulteriori informazioni:

Visualizzazione dell'elenco dei rapporti con il tag PCI (a pagina 282)
Ricerca di rapporti per un controllo PCI DDS specifico (a pagina 283)

Visualizzazione dell'elenco dei rapporti con il tag PCI

È possibile iniziare la valutazione della modalità di utilizzo dei rapporti CA User Activity Reporting Module per dimostrare la conformità a PCI visualizzando l'elenco dei rapporti predefiniti con il tag PCI.

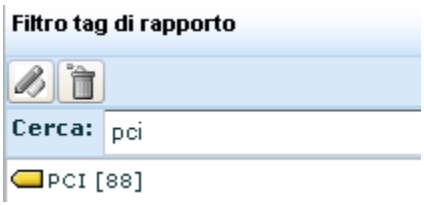
Per acquisire dimestichezza con i rapporti che dispongono del tag PCI

1. Fare clic sulla scheda Query e rapporti, quindi sulla sottoscheda Rapporti.

   Vengono visualizzati il filtro tag di rapporto e l'Elenco rapporti.

2. Inserire PCI nel campo Cerca.

   Viene visualizzato il tag PCI.



3. Rivedere gli elenchi di rapporti associati al tag PCI.

Ricerca di rapporti per un controllo PCI DDS specifico

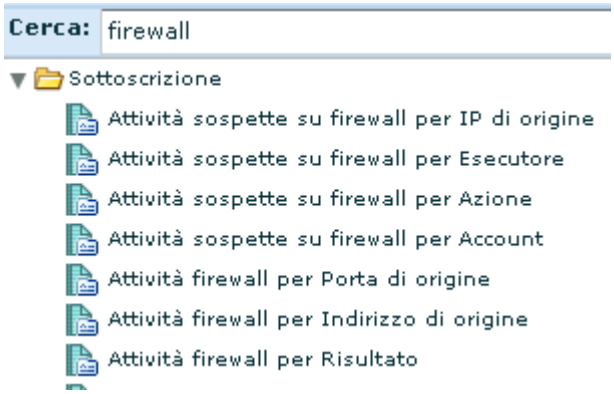
È possibile cercare rapporti predefiniti utilizzando le parole chiave relative a controlli PCI DDS specifici. La procedura seguente mostra alcuni esempi.

Nota: i numeri di riferimento sono i numeri associati al requisito PCI DDS cui si riferisce il rapporto.

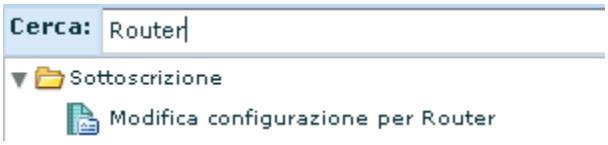
Per visualizzare l'elenco dei rapporti relativi ai controlli PCI DDS specifici

1. Fare clic sulla scheda Query e rapporti, quindi sulla sottoscheda Rapporti.
2. Per visualizzare il rapporto riguardante le modifiche alla configurazione del firewall (1.1.1), immettere Firewall come criterio di ricerca.

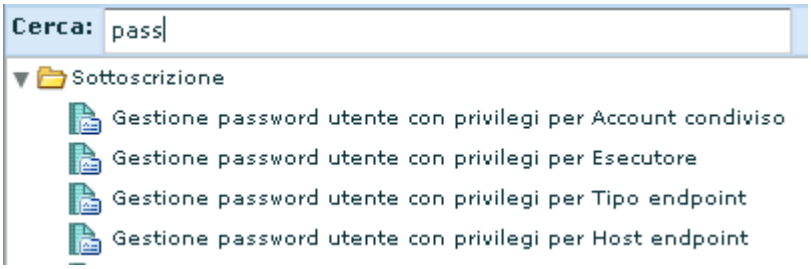
   Viene visualizzato un elenco di rapporti simile al seguente. Notare il rapporto denominato Modifiche di configurazione firewall.



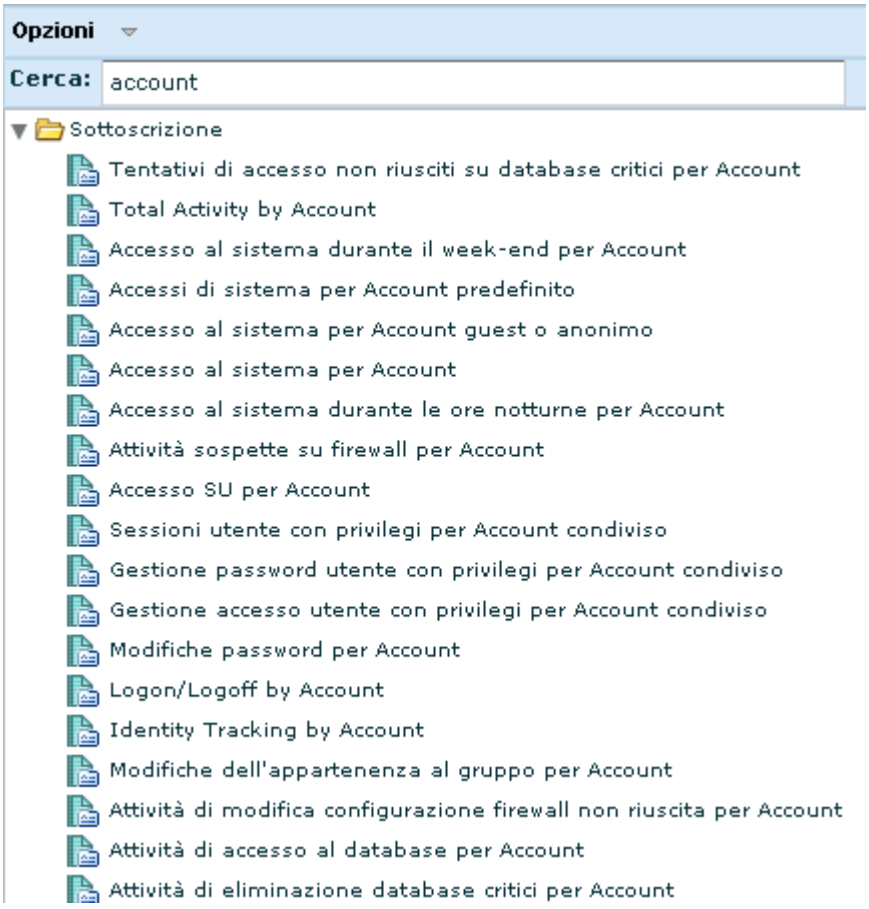
3. Per individuare il rapporto riguardante le modifiche alle configurazioni del router dopo aver verificato la sincronizzazione (1.3.6), immettere Router come criterio di ricerca.



4. Per individuare i rapporti riguardanti la gestione delle password (8.5), una delle potenti misure di controllo degli accessi, immettere Password come criterio di ricerca.



5. Per individuare i rapporti riguardanti aggiunte, modifiche e rimozioni degli account utente (12.5.4), una delle misure per il mantenimento di un criterio di protezione delle informazioni, immettere Account come criterio di ricerca.



Lavorare con un solo rapporto PCI

È possibile lavorare con qualsiasi rapporto, inclusi i rapporti PCI, nei seguenti modi:

- Visualizzare il rapporto selezionandone il nome dall'Elenco rapporti.
- Stampare il rapporto.
- Pianificare il rapporto, con l'opzione di invio ai destinatari selezionati.
- Visualizzare il processo di rapporto selezionato.
- Visualizzare il rapporto generato.

Per visualizzare o agire su un rapporto selezionato

1. Fare clic sulla scheda Query e rapporti e sulla sottoscheda Rapporti.
2. Selezionare Mostra rapporto selezionato nell'elenco a discesa Opzioni dell'Elenco rapporti, nel caso l'opzione non sia già selezionata.
3. Selezionare un nome rapporto dall'elenco.

   Il rapporto visualizza i risultati delle query, che in genere includono un riepilogo, la tendenza e i dettagli, nonché query specifiche del rapporto.
4. Per disattivare il caricamento di determinate query, scegliere Annulla.

5. Per stampare il rapporto visualizzato, fare clic su Stampa rapporto nel riquadro destro.

   Quando viene visualizzata la finestra di dialogo Stampa, selezionare una stampante e fare clic su Stampa.
6. Per pianificare la generazione di un rapporto da visualizzare in un momento successivo, fare clic su Pianifica rapporto.

   Viene visualizzata la procedura guidata Pianificazione rapporto e il rapporto compare nell'area Rapporti selezionati.
7. Immettere un nome di processo, ad esempio, Accesso alla risorsa per Host.

   Accettando tutti i valori predefiniti, il processo viene pianificato per l'esecuzione immediata senza ricorrenza e il rapporto viene generato in formato PDF senza notifiche di posta elettronica. I dati vengono estratti dal server corrente, dai peer e dai discendenti federati.
8. Fare clic su Salva, quindi su Chiudi.

9. Visualizzare il processo pianificato. Fare clic sulla scheda Rapporti pianificati, quindi sulla scheda secondaria Pianificazione rapporto.

   Viene visualizzato il processo appena pianificato.

Processi pianificati

	Nome processo	Abilitato	Server	Stato	Ricorrenza	Ora pianificata	Fuso orario	Autore	Formato
	Accesso alla risorsa per Host	true	caelm2	Pianificazione scaduta	Adesso	Martedì 28/09/2010 19:24:34	America/New_York	admin	PDF

10. Visualizzare il rapporto generato.
    a. Fare clic sulla scheda Rapporti pianificati, quindi sulla scheda secondaria Rapporti generati.
    b. (Facoltativo) Per limitare il numero di righe da visualizzare, selezionare un valore di ricorrenza diverso da Tutto oppure un intervallo di tempo relativo all'ultima ora.
    c. (Facoltativo) Fare clic su Aggiorna.
11. Dopo aver esaminato il rapporto generato, è possibile modificare il processo di rapporto per pianificarlo su base ricorrente. Procedere come indicato di seguito:
    a. Selezionare il rapporto generato dalla sottoscheda Pianificazione rapporto e fare clic su Modifica.
    b. Selezionare il passaggio Pianifica processi e selezionare l'opzione per la frequenza di occorrenza.
    c. Fare clic su Salva, quindi su Chiudi.

I prompt

Un prompt è un tipo speciale di query che consente di visualizzare i risultati in base al valore inserito e ai campi CEG selezionati dall'utente. Vengono restituite righe solo per gli eventi in cui il valore inserito dall'utente viene visualizzato in uno o più campi CEG selezionati.

Sui risultati delle query di prompt è possibile eseguire una qualsiasi delle seguenti azioni:

- Selezionare Mostra eventi non elaborati per sostituire la visualizzazione degli eventi perfezionati con l'evento non elaborato corrispondente e l'ora in cui esso si è verificato.
- Immettere una stringa nel campo Corrispondenza e selezionare Vai a per visualizzare solo le righe che contengono dati corrispondenti alla voce inserita dall'utente.
- Selezionare un'opzione di Esporta dati query per esportare i risultati della query in un documento PDF, in un foglio di calcolo di Excel o in un file XML.
- Selezionare Condizioni di risultato per filtrare la visualizzazione in base ad un intervallo di date specificato, per impostare il limite delle righe restituite o per cambiare la granularità dell'ora visualizzata. In alternativa, ripristinare le condizioni di risultato alle impostazioni predefinite.
- Selezionare Visualizza / Modifica filtri locali per definire filtri rapidi o avanzati.
- Stampare la query tramite la stampante locale selezionata.
- Aggiornare i dati di query manualmente oppure selezionando Aggiornamento automatico.

Utilizzo del Prompt di connettore

Ogni connettore configurato su un agente raccoglie eventi non elaborati da un'origine evento specifica, per poi inviarli all'archivio registro eventi di un server di raccolta di CA User Activity Reporting Module. Il processo di perfezionamento eventi converte gli eventi non elaborati in eventi perfezionati, per poi archiviarli nel server di rapporto di CA User Activity Reporting Module. Il prompt di connettore esegue una query sugli eventi del server di rapporto raccolti come eventi non elaborati dai connettori con il nome specificato dall'utente. I connettori possono avere un nome predefinito oppure un nome definito dall'utente. Copiare il nome del connettore da utilizzare e incollarlo nel campo del prompt di connettore, quindi fare clic su Vai a per visualizzare i risultati della query di prompt.

Utilizzare il prompt di connettore per:

- Visualizzare eventi da tutti i connettori basati sulla stessa integrazione. Ciò è possibile a condizione che si accetti il nome del connettore predefinito durante la distribuzione dei connettori.
- Verificare che un nuovo connettore stia recuperando eventi. Se più agenti dispongono di connettori con il nome specificato dall'utente, inserire il nome dell'agente nel campo Corrispondenza per restringere i risultati della query ai soli eventi recuperati dal nuovo connettore.

Per copiare il nome di un connettore attivo

1. Fare clic sulla scheda Amministrazione.

   Viene visualizzata Gestione raccolta log.

2. Fare clic su Explorer agente.

   Viene visualizzato Monitoraggio di stato agente, in cui i nomi del connettore vengono elencati in una colonna.

3. Fare clic col tasto destro del mouse sul connettore da utilizzare nella query di prompt e selezionare Copia nome connettore.

Per utilizzare il prompt di connettore

1. Fare clic su Query e rapporti.

   In Elenco query vengono visualizzate le cartelle Prompt, Sottoscrizione e, a volte, anche la cartella Utenti.

2. Espandere la cartella Prompt e selezionare Connettore.

   Il prompt di connettore visualizza il campo Connettore e il successivo campo CEG, che deve restare selezionato perché il prompt funzioni:

   agent_connector_name

   È il nome di un connettore.

3. Fare clic con il tasto destro del mouse nel campo Connettore e selezionare Incolla.

   Nel campo Connettore viene visualizzato il nome del connettore copiato da Monitoraggio di stato agente.

4. Fare clic su Vai a.

   Verranno visualizzati i risultati della query del prompt del connettore.

5. Utilizzare le seguenti descrizioni per interpretare i risultati della query:

   Gravità CA

   Indica la gravità dell'evento in cui i valori visualizzati in ordine crescente di gravità includono: Informazioni, Avviso, Impatto minimo, Impatto forte, Critico ed Errore irreversibile.

   Data

   Indica il momento in cui si è verificato l'evento.

   Categoria

   Identifica la categoria di alto livello dell'Azione evento corrispondente. Ad esempio, Accesso al sistema è la categoria per l'azione Autenticazione.

   Azione

   Identifica l'azione, laddove le azioni possibili sono determinate dalla classe dell'evento.

Nome agente

Identifica l'agente sul quale è in esecuzione il connettore.

Host

Identifica l'host di origine evento da cui il connettore esegue la raccolta di eventi.

Esecutore

Identifica l'attore di origine dell'evento, cioè l'identità che ha inizializzato l'azione. L'esecutore può essere espresso come nome utente di origine o come nome processo di origine.

Account

Identifica il nome utente dell'account utilizzato per l'autenticazione durante il tentativo da parte del connettore di connettersi all'host con l'origine evento da cui vengono raccolti gli eventi non elaborati. In genere, si tratta in questo caso di un tipo di account con privilegi ridotti. Le credenziali per questo account sono configurate sull'origine evento e sul sensore di registro del connettore.

Risultato

Specifica un codice relativo al risultato dell'evento dell'azione corrispondente, dove R sta per Riuscito, N per Non riuscito, A per Accettato, I per Interrotto, R per Rifiutato e S per Sconosciuto.

Nome connettore

Corrisponde al nome del connettore immesso nel campo del filtro prompt.

6. (Facoltativo) Selezionare Mostra eventi non elaborati.

   Il primo evento raccolto da un nuovo connettore si riferisce all'azione Avvio del sistema e termina con: result_string=<connector name> Connettore avviato correttamente.

Utilizzo del prompt Host

Si tratta delle query del prompt Host per gli eventi in cui il nome host specificato viene visualizzato nei campi CEG selezionati dell'evento perfezionato. Quando i dati dell'evento non elaborato vengono perfezionati, i dettagli dell'evento possono includere diversi nomi host CEG. Prendere in considerazione il seguente scenario:

1. Chi avvia l'evento su source_hostname tenta di eseguire un'azione, event_action, su una destinazione posizionata in dest_hostname.

   Nota: source_hostname e dest_hostname possono essere host diversi o il medesimo host.

2. L'evento viene registrato in un repository su event_source_hostname.

   Nota: Event_source_name può essere un host diverso da quello di source_hostname o dest_hostname, oppure il medesimo host.

3. Una copia dell'evento registrato su event_source_hostname viene generata da un agente CA User Activity Reporting Module che è stato installato su agent_hostname.

   Nota: agent_hostname è identico a event_source_name nella raccolta registri basata su agente, ma si differenzia da questo nella raccolta registri diretta e senza agente.

4. La copia dell'evento in event_logname viene trasmessa dall'agente CA User Activity Reporting Module su agent_hostname ad un server di raccolta CA User Activity Reporting Module.

Per utilizzare il prompt Host

1. Fare clic su Query e rapporti.

   L'Elenco query consente di visualizzare la cartella Prompt e una o più cartelle per le altre query.

2. Espandere Prompt e selezionare Host.

   Viene visualizzato il prompt Host.

3. Immettere il nome dell'host sul quale basare la query.

4. Selezionare i campi sui quali eseguire la query dei dati corrispondenti alla voce del nome host.

   source_hostname

   È il nome dell'host dove è stata avviata l'Azione evento.

   dest_hostname

   È il nome di un host che corrisponde alla destinazione dell'azione.

   event_source_hostname

   È il nome di un host che registra l'evento nel momento in cui esso si verifica.

   Ad esempio, è possibile distribuire un connettore basato su WinRm per raccogliere eventi dal Visualizzatore eventi su un host di Windows Server 2008. Per selezionare eventi recuperati da un determinato host di Windows Server 2008, immettere il nome host del server e selezionare questo campo.

   receiver_hostname

   Equivale ad agent_hostname.

   agent_hostname

   È il nome dell'host su cui viene distribuito un agente CA User Activity Reporting Module.

5. Fare clic su Vai a.

   Verranno visualizzati i risultati della query del prompt host.

6. Utilizzare le seguenti descrizioni per interpretare i risultati della query:

Gravità CA

Indica la gravità dell'evento in cui i valori visualizzati in ordine crescente di gravità includono: Informazioni, Avviso, Impatto minimo, Impatto forte, Critico ed Errore irreversibile.

Data

Indica il momento in cui si è verificato l'evento.

Utente di origine

Identifica il nome dell'utente su source_hostname che ha avviato l'Azione evento.

Risultato

Specifica un codice relativo al risultato dell'evento dell'azione corrispondente, dove R sta per Riuscito, N per Non riuscito, A per Accettato, I per Interrotto, R per Rifiutato e S per Sconosciuto.

Host agente

Identifica il nome dell'host su cui è installato l'agente CA User Activity Reporting Module che ha raccolto l'evento.

Host ricevente

È identico all'host agente.

Categoria

Identifica la categoria di alto livello dell'Azione evento corrispondente. Ad esempio, Accesso al sistema è la categoria per l'azione Autenticazione.

Azione

Identifica l'Azione evento eseguita dall'utente di origine.

Nome registro

Identifica il nome di registro utilizzato dal connettore che ha eseguito la raccolta dell'evento. Tutti i connettori basati sulla stessa integrazione trasmettono eventi in un file di registro riportando lo stesso nome di registro.

Utilizzo del prompt IP

Si tratta delle query del prompt IP per gli eventi in cui l'IP specificato viene visualizzato nei campi CEG selezionati dell'evento perfezionato. Quando i dati dell'evento non elaborato vengono perfezionati, i dettagli dell'evento includono diversi indirizzi IP di CEG. Prendere in considerazione il seguente scenario:

1. Chi avvia l'evento su source_address tenta di eseguire un'azione, event_action, su una destinazione che risiede in dest_address.

   Nota: source_address e dest_address possono essere diversi o identici.

2. L'evento viene registrato in un repository su event_source_address.

   Nota: event_source_address può essere diverso da source_address o dest_address, oppure può essere uguale ad uno di essi o a entrambi.

3. Un agente CA User Activity Reporting Module installato su agent_address genera una copia dell'evento registrato su event_source_address.

   Nota: agent_address è identico a event_source_address nella raccolta registri basata su agente, ma si differenzia da questo per la raccolta registri diretta e senza agente.

4. La copia dell'evento in event_logname viene trasmessa dall'agente CA User Activity Reporting Module su agent_address ad un server di raccolta CA User Activity Reporting Module.

Per utilizzare il prompt IP

1. Fare clic su Query e rapporti.

   L'Elenco query consente di visualizzare la cartella Prompt e una o più cartelle per le altre query.

2. Espandere la cartella Prompt e selezionare Host.

   Viene visualizzato il prompt IP.

3. Immettere l'indirizzo IP sul quale basare la query.

4. Selezionare uno o più campi per eseguire la query per i dati corrispondenti alla voce dell'indirizzo IP.

   source_address

   È il nome dell'indirizzo IP dell'host dove è stata avviata l'azione.

   dest_address

   È il nome dell'indirizzo IP di un host che corrisponde alla destinazione dell'azione.

event_source_address

È il nome dell'indirizzo IP di un host che registra l'evento non elaborato nel momento in cui si verifica.

Ad esempio, è possibile distribuire un connettore basato su WinRm per raccogliere eventi dal Visualizzatore eventi su un host di Windows Server 2008. Per selezionare eventi recuperati da un host specifico di Windows Server 2008, immettere l'indirizzo IP del server e selezionare questo campo.

receiver_hostaddress

Corrisponde ad agent_address.

agent_address

È l'indirizzo IP di un host sul quale viene distribuito l'agente CA User Activity Reporting Module.

5. Fare clic su Vai a.

   Verranno visualizzati i risultati della query del prompt IP.

6. Utilizzare le seguenti descrizioni per interpretare i risultati della query:

   Gravità CA

   Indica la gravità dell'evento in cui i valori visualizzati in ordine crescente di gravità includono: Informazioni, Avviso, Impatto minimo, Impatto forte, Critico ed Errore irreversibile.

   Data

   Indica il momento in cui si è verificato l'evento.

   Risultato

   Fornisce un codice per il risultato dell'azione corrispondente in cui la lettera visualizzata presenta i seguenti significati: R sta per riuscito, N per non riuscito, A per Accettato, I per Interrotto, R per Rifiutato e S per Sconosciuto.

   Porta di destinazione

   Identifica la porta di comunicazione sull'host di destinazione, cioè la destinazione dell'Azione evento.

IP origine

Identifica l'indirizzo IP dal quale è stata avviata l'Azione evento.

IP destinazione

Identifica l'indirizzo IP dell'host corrispondente alla destinazione dell'Azione evento.

IP di origine evento

Identifica l'indirizzo IP dell'host con il repository sul quale è stato inizialmente registrato l'evento.

IP agente

Identifica il nome dell'host con l'agente CA User Activity Reporting Module responsabile della raccolta di eventi dall'origine evento.

IP ricevente

È identico all'IP agente.

Categoria

Identifica la categoria di alto livello dell'Azione evento corrispondente. Ad esempio, Accesso al sistema è la categoria per l'azione Autenticazione.

Azione

Identifica l'Azione evento.

Nome registro

Identifica il nome registro utilizzato dal connettore che ha raccolto l'evento.

Utilizzo del prompt di Nome registro

Ciascun connettore basato sulla stessa integrazione restituisce al server di raccolta CA User Activity Reporting Module, in un file di registro e con un nome predefinito, i registri eventi raccolti dall'origine eventi. Il prompt del nome registro esegue una query per gli eventi relativi al nome registro specificato.

Utilizzare il prompt del nome registro per eseguire una query sugli eventi trasferiti in un file di registro con il nome specificato. Ciascun connettore è basato su un'integrazione. Ogni integrazione utilizza un nome registro predefinito. Una query eseguita per un nome registro specifico restituisce i risultati degli eventi raccolti da diversi agenti che utilizzano connettori basati sulla stessa integrazione o su una simile.

Per assegnare dei nomi ai registri, si utilizza una varietà di convenzioni:

- Nome integrazione. CA Federation è il nome registro per l'integrazione CA_Federation_Manager.
- Nome prodotto. McAfee Vulnerability Manager è il nome registro sia di McAfee_VM che di McAfee_VM_CM. MS AD Rights Management Services è il nome registro per Microsoft_Active_Directory_RMS e Microsoft_Active_Directory_RMS_ODBC.
- Nome fornitore: Oracle è il nome registro per Oracl10g, Oracle9i, Oracle_AppLog, e Oracle_Syslog.
- Tipo registro: Unix è il nome registro per le integrazioni seguenti: AIX_Syslog, HPUX_Syslog, Linux_Syslog, SLES_Syslog, e Solaris_Syslog.

Alcuni nomi registro vengono riutilizzati poiché vengono aggiunte nuove versioni o piattaforme. Ad esempio, NT-Security è il nome registro per i registri protezione relativi alle seguenti integrazioni: NTEventLog, Windows2k8 e WinRM.

Per utilizzare il prompt di Nome registro

1. Fare clic su Query e rapporti.

   L'Elenco query consente di visualizzare la cartella Prompt e una o più cartelle per le altre query.

2. Espandere la cartella Prompt e selezionare Nome registro.

   Viene visualizzato il filtro del prompt di Nome registro con il campo seguente:

   event_logname

   È il nome di un file di registro associato ad un'integrazione specifica.

3. Selezionare il nome registro utilizzato per la trasmissione degli eventi da visualizzare e fare clic su Vai a.

   Verranno visualizzati i risultati del prompt di nome registro.

4. Utilizzare le seguenti descrizioni per interpretare i risultati della query:

   Gravità CA

   Indica la gravità dell'evento in cui i valori visualizzati in ordine crescente di gravità includono: Informazioni, Avviso, Impatto minimo, Impatto forte, Critico ed Errore irreversibile.

   Data

   Indica il momento in cui si è verificato l'evento.

   Categoria

   Identifica la categoria di alto livello dell'Azione evento corrispondente. Ad esempio, Accesso al sistema è la categoria per l'azione Autenticazione.

   Azione

   Identifica l'Azione evento eseguita dall'esecutore corrispondente.

   Host

   Identifica l'host di origine evento da cui il connettore esegue la raccolta di eventi.

   Esecutore

   Identifica l'attore di origine dell'evento, cioè l'identità che ha inizializzato l'azione. L'esecutore può essere espresso come nome utente di origine o nome processo di origine.

Account

Identifica il nome utente dell'account utilizzato per l'autenticazione. Quando il connettore esegue un tentativo di connessione all'origine evento, si verifica l'autenticazione. Generalmente per l'autenticazione viene utilizzato un account con privilegi ridotti. Durante la distribuzione del connettore, l'amministratore configura sull'origine evento le credenziali per l'account, identificando quest'ultimo sul sensore di registro.

Risultato

Specifica un codice relativo al risultato dell'evento dell'azione corrispondente, dove R sta per Riuscito, N per Non riuscito, A per Accettato, I per Interrotto, R per Rifiutato e S per Sconosciuto.

Nome registro

Corrisponde al nome registro immesso nel campo relativo al filtro del prompt.

Utilizzo del prompt Porta

Sono le query del prompt Porta per gli eventi in cui la porta specificata viene visualizzata nei campi CEG selezionati dell'evento perfezionato. Quando i dati dell'evento non elaborato vengono perfezionati, i dettagli dell'evento includono diversi numeri di porta CEG. Prendere in considerazione il seguente scenario:

1. Tramite la porta di comunicazione in entrata dest_port, l'iniziatore dell'evento sull'host di origine utilizza la porta di comunicazione in uscita source_port per avviare l'Azione evento su una destinazione che risiede sull'host di destinazione.

   Nota: source_port e dest_port sono identiche per gli eventi locali. In caso contrario, saranno specifiche dell'host.

2. L'evento viene registrato in un repository sull'origine evento.
3. Un agente CA User Activity Reporting Module genera una copia dell'evento registrato sull'origine evento.
4. Tramite la porta di uscita receiver_port, l'agente trasmette sul server di raccolta CA User Activity Reporting Module una copia dell'evento.

   Nota: per garantire le comunicazioni sul server di raccolta CA User Activity Reporting Module, l'agente utilizza la porta 17001.

Per utilizzare il prompt Porta

1. Fare clic su Query e rapporti.

   L'Elenco query consente di visualizzare la cartella Prompt e una o più cartelle per le altre query.

2. Espandere la cartella Prompt e selezionare Porta.

   Viene visualizzato il prompt Porta.

3. Immettere il numero di porta sul quale basare la query.

4. Selezionare i campi sui quali far eseguire la query dei dati corrispondenti alla voce del numero di porta:

   source_port

   È la porta di comunicazione utilizzata per inizializzare l'azione.

   dest_port

   Corrisponde alla porta di comunicazione sull'host di destinazione , cioè la destinazione dell'azione.

   receiver_port

   È la porta utilizzata dall'agente per comunicare con il server di raccolta CA User Activity Reporting Module.

5. Fare clic su Vai a.

   Verranno visualizzati i risultati della query del prompt Porta.

6. Utilizzare le seguenti descrizioni per interpretare i risultati della query:

   Gravità CA

   Indica la gravità dell'evento in cui i valori visualizzati in ordine crescente di gravità includono: Informazioni, Avviso, Impatto minimo, Impatto forte, Critico ed Errore irreversibile.

   Data

   Indica il momento in cui si è verificato l'evento.

   IP origine

   Identifica l'indirizzo IP dell'host dal quale è stata avviata l'Azione evento.

   Risultato

   Specifica un codice relativo al risultato dell'evento dell'azione corrispondente, dove R sta per Riuscito, N per Non riuscito, A per Accettato, I per Interrotto, R per Rifiutato e S per Sconosciuto.

Porta di origine

Identifica la porta di uscita utilizzata per avviare l'azione.

Porta di destinazione

Identifica la porta di entrata sull'host di destinazione.

Host ricevente

Identifica la porta di uscita sull'agente utilizzato per inviare registri evento al server CA User Activity Reporting Module.

Categoria

Identifica la categoria di alto livello dell'Azione evento corrispondente. Ad esempio, Accesso al sistema è la categoria per l'azione Autenticazione.

Azione

Identifica l'Azione evento.

Nome registro

Identifica il nome registro utilizzato dal connettore che ha raccolto l'evento.

Utilizzo del prompt Utente

Ciascun evento fornisce informazioni su due attori: l'Origine e la Destinazione.

- L'attore di Origine avvia l'azione che determina il verificarsi dell'evento.

  L'attore di origine può essere un utente, source_username, oppure un processo, source_processname.

- La destinazione o l'attore di Destinazione, indicato con "dest", corrisponde alla destinazione dell'azione.

  L'attore di destinazione può essere un utente, dest_username, oppure un oggetto, dest_objectname.

Il prompt Utente esegue le query per gli eventi in cui l'attore specificato viene visualizzato nei campi CEG selezionati dell'evento perfezionato. Prendere in considerazione il seguente scenario:

1. L'attore di origine, source_username o source_processname, tenta di eseguire un'azione sull'attore di destinazione, destination_username o destination_objectname.
2. L'evento viene registrato in un repository sull'origine evento.
3. Un agente CA User Activity Reporting Module genera una copia dell'evento registrato sull'origine evento e lo trasmette ad un server CA User Activity Reporting Module.

Per utilizzare il prompt Utente

1. Fare clic su Query e rapporti.

   L'Elenco query consente di visualizzare la cartella Prompt e una o più cartelle per le altre query.
2. Espandere la cartella Prompt e selezionare Porta.

   Viene visualizzato il prompt Utente.
3. Immettere il nome dell'utente sul quale basare la query.
4. Selezionare i campi sui quali eseguire la query dei dati corrispondenti al nome utente.

   source_username

   Indica il nome dell'utente che ha avviato l'Azione evento.

   dest_username

   Indica il nome dell'utente che rappresenta la destinazione dell'azione.

   source_objectname

   Indica il nome dell'oggetto coinvolto nell'azione espressa nelle informazioni evento.

   dest_objectname

   Indica il nome dell'oggetto che rappresenta la destinazione dell'azione
5. Fare clic su Vai a.

   Verranno visualizzati i risultati della query del prompt Utente.

6. Utilizzare le seguenti descrizioni per interpretare i risultati della query:

Gravità CA

Indica la gravità dell'evento in cui i valori visualizzati in ordine crescente di gravità includono: Informazioni, Avviso, Impatto minimo, Impatto forte, Critico ed Errore irreversibile.

Data

Indica il momento in cui si è verificato l'evento.

Host di destinazione

Identifica il nome dell'host con l'utente che rappresentava la destinazione dell'Azione evento.

Risultato

Specifica un codice relativo al risultato dell'evento dell'azione corrispondente, dove R sta per Riuscito, N per Non riuscito, A per Accettato, I per Interrotto, R per Rifiutato e S per Sconosciuto.

Utente di origine

Identifica l'utente che ha inizializzato l'Azione evento.

Oggetto di origine

Identifica l'oggetto sull'host di origine coinvolto nell'Azione evento.

Utente di destinazione

Identifica l'utente che rappresentava la destinazione dell'Azione evento.

Oggetto di destinazione

Identifica l'oggetto sull'host di origine coinvolto nell'Azione evento.

Categoria

Identifica la categoria di alto livello dell'Azione evento corrispondente. Ad esempio, Accesso al sistema è la categoria per l'azione Autenticazione.

Azione

Identifica l'Azione evento.

Nome registro

Identifica il nome registro utilizzato dal connettore che ha raccolto l'evento.

Come creare una query

È possibile creare query personalizzate utilizzando la procedura guidata Progettazione query. Quando si crea una query è necessario stabilire se applicarla al database eventi, al database incidenti o al database ODBC. Il database eventi consente di archiviare le informazioni relative a tutti gli eventi ricevuti da tale server. Il database incidenti consente di archiviare le informazioni relative agli incidenti e agli elementi di evento dei componenti corrispondenti in base a quanto specificato dalle regole di correlazione.

È possibile eliminare query personalizzate ed esportare le informazioni corrispondenti. È inoltre possibile copiare una query di sottoscrizione per creare una query personalizzata e modificare tale query mediante la procedura guidata di progettazione delle query. Solo gli utenti con ruolo di amministratore o analista possono creare, eliminare o modificare le query.

La creazione di una query utilizzando la procedura guidata Progettazione query comprende i seguenti passaggi:

1. Apertura della procedura guidata Progettazione query.
2. Aggiunta di informazioni relative all'identità e ai tag, compresa la specificazione del database di destinazione.
3. Selezione delle colonne di query.
4. (Facoltativo) Impostazione delle condizioni e dei filtri per la query.
5. Impostazione dell'intervallo di date e delle condizioni dei risultati.
6. (Facoltativo) Scelta delle opzioni di visualizzazione per le query.
7. (Facoltativo) Aggiunta di valori drill-down per la query.

Ulteriori informazioni:

Apertura della procedura guidata Progettazione query (a pagina 306)
Aggiunta di dettagli sulla query (a pagina 307)
Aggiunta di colonne di query (a pagina 309)
Aggiunta di colonne di query ODBC (a pagina 311)
Impostazione dei filtri della query (a pagina 314)
Aggiunta di un rapporto drill-down (a pagina 324)
Creazione di una visualizzazione di query (a pagina 323)

Apertura della procedura guidata Progettazione query

Per creare una nuova query personalizzata, creare una copia della query o modificarne una esistente, è necessario avviare la procedura guidata Progettazione query.

Per aprire la procedura guidata Progettazione query

1. Fare clic sulla scheda Query e rapporti, quindi sulla sottoscheda Query.

   Viene visualizzato l'Elenco query.

2. Fare clic su Opzioni e scegliere Nuovo.

   Viene visualizzata la procedura guidata Progettazione query.

   Mentre si utilizza la procedura guidata:

   - Fare clic su Salva per salvare la query senza chiudere la procedura.
   - Fare clic su Salva e chiudi per salvare la query e chiudere la procedura.
   - Fare clic su Ripristina per ripristinare la visualizzazione della procedura alle ultime impostazioni salvate.

Ulteriori informazioni

Creazione di una visualizzazione di query (a pagina 323)
Aggiunta di un rapporto drill-down (a pagina 324)

Aggiunta di dettagli sulla query

Il primo passaggio della creazione di una query consiste nell'immissione delle informazioni di identificazione e nell'impostazione degli eventuali tag da includere.

Per aggiungere una nuova query

1. Aprire la procedura guidata Progettazione query.
2. Digitare un nome per la query (obbligatorio) e un nome breve (facoltativo) da utilizzare nei rapporti. Se una query è inclusa in un rapporto, il nome breve corrispondente verrà visualizzato soltanto nel riquadro della query.
3. Selezionare il tipo di connessione desiderato. Il valore UARM predefinito viene visualizzato nell'elenco a discesa assieme ai nomi delle connessioni ODBC impostate nell'area Servizio di rapporto.

   UARM predefinito

   Indirizza la query ai database di eventi o di incidenti interni.

   Connessioni ODBC

   Indirizza la query a una tabella ODBC esterna selezionata. L'elenco a discesa Tabella viene compilato con le visualizzazioni contenute nel database di destinazione.
4. Selezionare la tabella a cui si desidera applicare la query:

   Se è stato selezionato il valore UARM predefinito, selezionare uno dei seguenti elementi:

   Evento

   Applica la query al database eventi, il quale archivia tutte le informazioni evento non elaborate e perfezionate ricevute dal server corrente, o disponibili mediante la federazione.

   Incidente

   Applica la query al database incidenti, il quale archivia gli incidenti creati dal sistema di correlazione eventi e le informazioni evento utilizzate per creare gli incidenti. Le regole di correlazione consentono di verificare i componenti specifici di un evento utilizzato per la creazione di un incidente.

   Se è stata selezionata una connessione personalizzata, selezionare la tabella ODBC desiderata. L'elenco verrà popolato in base alle tabelle della connessione ODBC selezionata.
5. Digitare le eventuali note di progettazione nel campo Descrizione.

Nota: è consigliabile utilizzare questo campo per informazioni relative alla struttura della query. È ad esempio possibile inserire una spiegazione del motivo per cui la query contiene determinati campi e funzioni.

6. Selezionare uno o più tag cui si vuole associare la query utilizzando il Controllo pilota tag.
7. (Facoltativo) Per aggiungere un tag di categoria personalizzato, inserire un nome tag nel campo di immissione Aggiungi tag personalizzato e fare clic sul pulsante Aggiungi tag.

   Nel Controllo pilota tag viene visualizzato il tag personalizzato, già selezionato.
8. (Facoltativo) Per aggiungere un tag personalizzato nidificato, selezionare un tag oppure digitare il nome del tag padre seguito da una barra rovesciata, quindi digitare il nome del tag figlio. Quindi selezionare Aggiungi tag. Ad esempio, è possibile digitare: "Normative\Standard del settore". È possibile aggiungere ulteriori tag, mantenendo il formato a\b\c e così via.

   Nota: se si elimina uno dei tag nidificati personalizzati, verranno eliminati anche tutti i tag personalizzati in cui è nidificato, compreso il tag padre. Se si nidifica un tag personalizzato all'interno di un tag di sottoscrizione e quindi lo si elimina, verranno eliminati solo i tag personalizzati.

   Una volta completato il processo, il nuovo tag viene visualizzato nell'elenco, con i tag personalizzati nidificati visibili quando si espande il tag padre.
9. Fare clic sulla freccia corrispondente per accedere al passaggio di progettazione della query che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, la nuova query viene visualizzata nell'Elenco query; altrimenti, verrà visualizzato il passaggio selezionato della procedura guidata.

Aggiunta di colonne di query

Per creare una query a livello di database di incidenti o di eventi, scrivere un'istruzione SQL in grado di ottenere le informazioni sull'evento dal deposito eventi di log. La procedura guidata di progettazione delle query consente di automatizzare questo procedimento.

Per creare un'istruzione SQL per le query

1. Aprire la procedura guidata Progettazione query.
2. Inserire il nome ed il tag, se non ancora specificati, e procedere al passaggio Colonne query.
3. (Facoltativo) Selezionare la casella di controllo Solo eventi unici.
4. Impostare le colonne CEG che si desidera interrogare facendo clic sul pulsante Aggiungi nella parte superiore del riquadro. Le colonne verranno visualizzate in base all'ordine di aggiunta. È possibile modificare l'ordine utilizzando i pulsanti Giù e Su situati nella parte superiore del riquadro.
5. Selezionare le impostazioni desiderate per ogni colonna, tra cui:

   Visualizza nome

   Consente di inserire un nome diverso per la colonna, una volta visualizzata in formato Tabella o Visualizzatore eventi. Se non viene immesso alcun nome, come nome di colonna verrà utilizzato il nome del campo nativo, ad esempio "event_count".

   Funzione

   Consente di applicare una delle seguenti funzioni SQL ai valori della colonna:

   - COUNT: restituisce il numero totale di eventi.
   - AVG: restituisce la media dei valori event_count. La funzione è disponibile soltanto per i campi event_count.
   - SUM: restituisce la somma dei valori event_count. La funzione è disponibile soltanto per i campi event_count.
   - TRIM: rimuove tutti gli spazi nella stringa di testo relativa alla query.

- TOLOWER: converte in minuscolo la stringa di testo della query.
- TOUPPER: converte in maiuscolo la stringa di testo della query.
- MIN: restituisce il valore degli eventi più basso.
- MAX: restituisce il valore degli eventi più elevato.
- UNIQUECOUNT: restituisce il numero di eventi univoci.

Ciascun campo CEG appartiene a uno dei seguenti tipi: stringa, numero intero o valore data/ora. Quando viene aggiunto un campo CEG a una query, CA User Activity Reporting Module consente di creare funzioni applicabili al tipo disponibile corrispondente. Ad esempio, se si seleziona ideal_model, verranno visualizzate soltanto le funzioni applicabili ai valori della stringa.

Ordine gruppo

Consente di impostare la visualizzazione di query in modo da mostrare le colonne selezionate raggruppate in base all'attributo selezionato. Ad esempio, è possibile impostare la query in modo da raggruppare gli eventi in base al nome origine. È possibile controllare l'ordine in cui viene applicato alle varie colonne. Se i valori della prima colonna sono identici, verranno applicati i secondi. Ad esempio, è possibile raggruppare più eventi dalla stessa origine in base al nome utente.

Ordinamento

Consente di controllare l'ordine dei valori selezionati. È possibile controllare l'ordine in cui viene applicato alle varie colonne. Se i valori della prima colonna sono identici, verranno applicati i secondi.

Decrescente

Consente di impostare i valori delle colonne in modo da visualizzarli in ordine decrescente (dal valore più elevato a quello più basso) anziché nell'ordine crescente predefinito.

Non null

Controlla se la riga viene visualizzata in una tabella o nel Visualizzatore eventi se non contiene alcun valore. La selezione della casella di controllo Non null rimuove la riga dal risultato della query in caso essa non contenga valori visualizzabili.

Visibile

Controlla se la colonna è visualizzata in una tabella o nel formato Visualizzatore eventi. È possibile utilizzare questa impostazione per rendere disponibili i dati delle colonne nella visualizzazione dei dettagli senza mostrarli nella visualizzazione stessa.

Nota: quando si seleziona una funzione diversa da TRIM, TOLOWER, TOUPPER o un'impostazione di ordine di gruppo per una colonna, è necessario selezionare la stessa impostazione anche per le altre colonne. In caso contrario, CA User Activity Reporting Module visualizzerà un messaggio di errore.

6. (Facoltativo) Utilizzare le frecce rivolte verso l'alto e verso il basso nella parte superiore del riquadro Colonne selezionate per modificare l'ordine delle colonne secondo necessità.
7. Fare clic sulla freccia corrispondente per accedere al passaggio di progettazione della query che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, la nuova query viene visualizzata nell'Elenco query; altrimenti, verrà visualizzato il passaggio selezionato della procedura guidata.

Ulteriori informazioni:

Come creare una query (a pagina 305)
Aggiunta di colonne di query ODBC (a pagina 311)

Aggiunta di colonne di query ODBC

Per creare una query, scrivere un'istruzione in grado di ottenere dal database ODBC di destinazione le informazioni di evento desiderate. La procedura guidata di progettazione delle query consente di automatizzare questo procedimento.

Procedere come descritto di seguito:

1. Aprire la procedura guidata Progettazione query.
2. Inserire il nome ed il tag, se non ancora specificati, e procedere al passaggio Colonne query.
3. (Facoltativo) Selezionare la casella di controllo Solo eventi unici.

4. Impostare le colonne che si desidera interrogare facendo clic sul pulsante Aggiungi nella parte superiore del riquadro. Le colonne verranno visualizzate in base all'ordine di aggiunta. È possibile modificare l'ordine utilizzando i pulsanti Giù e Su situati nella parte superiore del riquadro.
5. Selezionare le impostazioni desiderate per ogni colonna, tra cui:

   Visualizza nome

   Consente di inserire un nome diverso per la colonna, una volta visualizzata in formato Tabella o Visualizzatore eventi. Se non viene immesso alcun nome, il nome della colonna corrisponderà al nome del campo nativo.

   Funzione

   Consente di applicare una funzione ai valori della colonna. Ciascun campo appartiene a uno dei seguenti tipi: stringa, numero intero o valore data/ora. Quando viene aggiunta una colonna a una query, CA User Activity Reporting Module visualizza soltanto le funzioni applicabili al tipo corrispondente.

   Ordine gruppo

   Consente di impostare la visualizzazione di query in modo da mostrare le colonne selezionate raggruppate in base all'attributo selezionato. Ad esempio, è possibile impostare la query in modo da raggruppare gli eventi in base al nome origine. È possibile controllare l'ordine in cui viene applicato alle varie colonne. Se i valori della prima colonna sono identici, verranno applicati i secondi. Ad esempio, è possibile raggruppare più eventi dalla stessa origine in base al nome utente.

   Ordinamento

   Consente di controllare l'ordine dei valori selezionati. È possibile controllare l'ordine in cui viene applicato alle varie colonne. Se i valori della prima colonna sono identici, verranno applicati i secondi.

   Decrescente

   Consente di impostare i valori delle colonne in ordine decrescente (dal valore maggiore a quello minore).

   Non null

   Controlla se la riga viene visualizzata in una tabella o nel Visualizzatore eventi se non contiene alcun valore. La selezione della casella di controllo Non null rimuove la riga dal risultato della query in caso essa non contenga valori visualizzabili.

Visibile

Controlla se la colonna è visualizzata in una tabella o nel formato Visualizzatore eventi. È possibile utilizzare questa impostazione per rendere disponibili i dati delle colonne nella visualizzazione dei dettagli senza mostrarli nella visualizzazione stessa.

Nota: quando si seleziona una funzione diversa da TRIM, TOLOWER, TOUPPER o un'impostazione di ordine di gruppo per una colonna, è necessario selezionare la stessa impostazione anche per le altre colonne. In caso contrario, CA User Activity Reporting Module visualizzerà un messaggio di errore.

6. (Facoltativo) Utilizzare le frecce rivolte verso l'alto e verso il basso nella parte superiore del riquadro Colonne selezionate per modificare l'ordine delle colonne secondo necessità.
7. Fare clic sulla freccia corrispondente per accedere al passaggio di progettazione della query che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Dopo aver fatto clic su Salva e chiudi, la nuova query verrà visualizzata nell'Elenco query. In caso contrario verrà visualizzato il passaggio selezionato della procedura guidata.

Ulteriori informazioni:

Come creare una query (a pagina 305)
Aggiunta di colonne di query (a pagina 309)

Impostazione dei filtri della query

È possibile filtrare le informazioni restituite dalla query utilizzando filtri semplici o avanzati. I filtri semplici consentono di creare istruzioni di filtro semplice applicabili ai database CA User Activity Reporting Module predefiniti. I filtri avanzati consentono di creare istruzioni più complesse, comprese le istruzioni nidificate. I filtri avanzati possono essere applicati alle query interne o alle query ODBC esterne.

Per impostare i filtri delle query

1. Aprire la procedura guidata Progettazione query.
2. Inserire il nome e il tag, se non già specificato, e proseguire fino al passaggio Filtri query.

   Viene visualizzata la finestra di dialogo Filtri query, in cui è disponibile la scheda Filtri semplici.

   Nota: i filtri semplici non sono disponibili se durante la creazione di una query viene selezionata una connessione personalizzata. Per qualificare una query ODBC personalizzata, utilizzare i filtri avanzati.
3. Creare i filtri semplici desiderati per ricercare i valori del campo CEG specificati.
4. Fare clic sulla scheda Filtri avanzati.
5. Creare i filtri avanzati desiderati.
6. Fare clic sulla freccia corrispondente per accedere al passaggio di progettazione della query che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Facendo clic su Salva e chiudi, la nuova query viene visualizzata nell'Elenco query; altrimenti, verrà visualizzato il passaggio Progettazione query selezionato.

Ulteriori informazioni:

Creazione di un filtro evento semplice (a pagina 315)
Creazione di un filtro di eventi avanzato (a pagina 315)
Utilizzo di filtri avanzati (a pagina 316)

Creazione di un filtro evento semplice

È possibile creare filtri semplici per impostare parametri di ricerca per valori comuni. Ad esempio, si potrebbe impostare il campo Modello ideale su "Amministrazione contenuti" per identificare tutti gli eventi con quel valore nel campo CEG Modello ideale. I filtri semplici vengono utilizzati da molte funzionalità, incluse le query di evento o incidente, le regole di soppressione e aggregazione e le regole di inoltro degli eventi.

Per creare un filtro semplice

1. Selezionare la casella di controllo per qualsiasi campo o campi di filtro semplice che si desidera definire, quindi selezionare un valore nell'elenco a discesa oppure immettere il valore desiderato nel campo di immissione del testo.
2. Dopo aver aggiunto tutti i filtri semplici desiderati, fare clic su Salva.

Ulteriori informazioni

Utilizzo di filtri avanzati (a pagina 584)
Creazione di un filtro di eventi avanzato (a pagina 586)

Creazione di un filtro di eventi avanzato

I filtri avanzati vengono utilizzati da molte funzioni, tra cui la creazione di query, la pianificazione di rapporti, i processi di avviso e i filtri locali e globali.

Per creare un filtro avanzato

1. Se si sta creando un processo di rapporto pianificato o un processo di avviso, fare clic sulla scheda Eventi o Incidenti per impostare il tipo di filtro appropriato. Poiché un processo di rapporto o di avviso può contenere sia query di evento che query di incidente, è possibile impostare i tipi di filtro separatamente.
2. Fare clic su Nuovo filtro evento.

   La prima riga della tabella dei filtri degli eventi diventa attiva e nelle relative colonne Logico e Operatore vengono visualizzati, rispettivamente, i valori predefiniti "And" e "Equal to".
3. Fare clic sulla cella Logico e modificare il valore logico secondo necessità.
4. Fare clic sulla cella Colonna, quindi selezionare la colonna relativa alle informazioni sugli eventi desiderata dal menu a discesa.

5. Fare clic sulla cella Operatore, quindi selezionare l'operatore desiderato dal menu a discesa.
6. Fare doppio clic sulla cella Valore, quindi immettere il valore desiderato.
7. (Facoltativo) Fare doppio clic sulle celle relative alle parentesi aperte e chiuse ed immettere il numero di parentesi necessarie.
8. (Facoltativo) Ripetere i passaggi da 1 a 6 secondo necessità per aggiungere ulteriori istruzioni dei filtri.
9. Una volta immesse le istruzioni dei filtri desiderate, fare clic su Salva.

Ulteriori informazioni:

Creazione di un filtro evento semplice (a pagina 584)
Utilizzo di filtri avanzati (a pagina 584)

Utilizzo di filtri avanzati

È possibile utilizzare filtri avanzati per definire eventuali funzioni per l'esecuzione di query sul database, tra cui la restrizione delle query o l'aggiunta di ulteriori qualifiche ai filtri semplici. L'interfaccia Filtri avanzati contiene un modulo per l'immissione di colonne, operatori e valori logici in funzione dei requisiti di filtro.

Nota: la presente sezione contiene una breve descrizione dei termini utilizzati nei filtri avanzati. Per sfruttare al massimo i filtri avanzati, è necessario disporre di una conoscenza approfondita della terminologia dei filtri e della Grammatica evento comune (CEG).

I termini elencati di seguito vengono usati per unire più istruzioni di filtro:

And

Consente di visualizzare le informazioni sugli eventi se *tutti* i termini associati risultano veri.

Oppure

Consente di visualizzare le informazioni sugli eventi se *uno* dei termini associati risulta vero.

Having

Consente di perfezionare i termini dell'istruzione principale tramite l'aggiunta di un'istruzione di qualificazione. Ad esempio, è possibile impostare filtri avanzati e aggiungere un'istruzione "having" per restituire da quegli host soltanto eventi di un livello di gravità specifico.

I filtri avanzati utilizzano i seguenti operatori per la creazione di condizioni di base:

Operatori relazionali

Comprendono le informazioni sugli eventi se sussiste la relazione appropriata tra la colonna e il valore immesso. Sono disponibili i seguenti operatori relazionali:

- Uguale a
- Diverso da
- Minore di
- Maggiore di
- Minore o uguale a
- Maggiore o uguale a

Ad esempio, l'operatore *Maggiore di* include le informazioni sugli eventi dalla colonna selezionata se il relativo valore è maggiore del valore impostato.

Simile

Include le informazioni sugli eventi se la colonna contiene uno schema immesso, utilizzando % per impostare lo schema desiderato. Ad esempio, L% restituisce i valori che iniziano con L, %L% restituisce i valori in cui L rappresenta la prima o l'ultima lettera.

Non uguale

Include le informazioni sugli eventi se la colonna non contiene lo schema specificato.

Nel set

Include le informazioni di evento se la colonna contiene uno più valori del set delimitato da virgole immesso dall'utente. Se nel set sono presenti più valori, essi devono essere separati da virgole.

Non in set

Include le informazioni di evento se la colonna non contiene uno più valori del set delimitato da virgole immesso dall'utente. Se nel set sono presenti più valori, essi devono essere separati da virgole.

Corrisponde a

Include le informazioni di evento corrispondenti ad uno o più caratteri immessi, consentendo di eseguire una ricerca per parola chiave. Il valore Corrisponde a non è disponibile per tutte le query ODBC.

Con chiave

Comprende le informazioni di evento impostate come valore chiave durante la configurazione del server di rapporto. È possibile utilizzare valori chiave per impostare la rilevanza per l'azienda o altri gruppi organizzativi.

Senza chiave

Comprende le informazioni di evento non impostate come valore chiave durante la configurazione del server di rapporto. È possibile utilizzare valori chiave per impostare la rilevanza per l'azienda o altri gruppi organizzativi.

Modalità di impostazione delle condizioni risultato

È possibile impostare un intervallo di date e altre condizioni risultato per la query, tra cui i limiti di righe e il periodo di tempo della visualizzazione di base. È possibile modificare le condizioni dei risultati in qualsiasi momento, nonché modificare le query in base alle proprie esigenze senza modificare la query di base o i filtri corrispondenti.

Se viene creato un rapporto pianificato o un alert, è possibile impostare le condizioni di risultato sia per le query di evento che per le query di incidente che costituiscono il processo.

È possibile impostare i seguenti tipi di condizioni di risultato:

- Condizioni dell'intervallo date che regolano la durata della ricerca delle query.
- Condizioni di visualizzazione, come il numero massimo di righe. È possibile utilizzare un sottoinsieme limitato di condizioni di visualizzazioni mediante query ODBC personalizzate.
- Condizioni degli eventi raggruppati, come gli eventi raggruppati più recenti dopo una data precisa, o gli eventi raggruppati che contengono un dato numero di eventi. Le condizioni degli eventi raggruppati non sono disponibili per le query ODBC personalizzate.

  Nota: se durante la creazione di una query non viene raggruppata almeno una colonna, gli utenti non saranno in grado di modificare le condizioni di risultato della visualizzazione della query.

Impostazione di un intervallo di ora o di data

È possibile impostare una condizione di intervallo di ora o data per la query. Questo migliora l'efficienza della query restringendo la parte del deposito eventi di log in cui deve effettuare la ricerca.

È possibile utilizzare un intervallo data/ora predefinito oppure crearne uno personalizzato. È necessario impostare un'ora di inizio e un'ora di fine per un intervallo di tempo personalizzato. Se viene impostato un solo parametro, questo viene espresso come una clausola "Where".

Per impostare le condizioni risultato

1. Aprire la finestra di dialogo Condizioni risultato.
2. Se si sta creando un processo di rapporto pianificato o un processo di alert, fare clic sulla scheda Eventi o Incidenti per impostare il tipo di filtro appropriato. Poiché un processo di rapporto o di avviso può contenere sia query di evento che query di incidente, è possibile impostare i tipi di filtro separatamente.
3. Selezionare un intervallo data/ora predefinito nell'elenco a discesa. Se si crea una query ODBC personalizzata, sarà necessario selezionare anche la colonna data/ora se si desidera utilizzare la query come riferimento.

   Nota: se si sta creano un alert o un rapporto pianificato, l'interfaccia visualizza gli intervalli di tempo predefiniti seguenti:

   - Alert: i 5 minuti precedenti
   - Rapporto pianificato: le 6 ore precedenti
4. (Facoltativo) Per creare un intervallo data/ora personalizzato, seguire questi passaggi secondari:

   a. Fare clic su Modifica accanto al campo di immissione "Ora di fine dinamica" nell'area Selezione intervallo date. Questo permette di impostare la fine del periodo di tempo nel quale si desidera che la query esegua la ricerca.

      Verrà visualizzata la finestra di dialogo Specifica tempo dinamico.

   b. Selezionare l'ora di riferimento da usare come base per il parametro e fare clic su Aggiungi.

   c. Selezionare il parametro di ora desiderato e fare clic su Aggiungi. È possibile aggiungere più parametri orari.

   d. Al termine della procedura di aggiunta dei parametri, fare clic su OK.

La finestra di dialogo Specifica tempo dinamico viene chiusa e i valori selezionati verranno visualizzati nell'area Ora di fine dinamica. Se si usano più parametri, essi formano una descrizione di tempo completa, dove ciascun parametro fa riferimento al primo. Ad esempio, se all'area Ora di fine dinamica vengono aggiunti i valori Inizio del mese e Giorno della settimana - Martedì, la query terminerà il primo martedì del mese.

Nota: quando si usano valori del tipo Numero di, come Numero di giorni o Numero di ore, è necessario specificare un numero *negativo* per impostare un periodo passato. L'uso di un numero positivo implica l'impostazione di un'ora di fine futura e fa sì che la query continui a inviare risultati fino a quando nel deposito eventi di log è presente almeno un evento qualificato.

Ad esempio, se nell'area Ora di fine dinamica vengono aggiunti i valori "adesso" e "numero di minuti - 10", la query verrà avviata 10 minuti prima dell'ora di fine selezionata.

e. Ripetere il passaggio 2 nell'area Ora di fine dinamica per impostare l'inizio dell'intervallo data/ora su cui eseguire la ricerca.

Se non si specifica un intervallo di date, la query viene applicata a tutti gli eventi del deposito eventi di log. Se si specifica un intervallo di date non valido, la query non restituisce alcun risultato.

5. Fare clic sulla freccia corrispondente per accedere al passaggio di progettazione della query che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, la nuova query viene visualizzata nell'Elenco query; altrimenti, verrà visualizzato il passaggio selezionato della procedura guidata.

Impostazione delle condizioni di visualizzazione e raggruppamento

È possibile impostare condizioni che consentono di controllare la visualizzazione delle query e le condizioni per la ricerca di eventi in base alle modalità di raggruppamento. Se vengono impostate le condizioni per una query ODBC personalizzata, saranno disponibili soltanto le opzioni Limite riga e Nessun limite.

Per impostare le condizioni di visualizzazione e raggruppamento

1. Aprire la finestra di dialogo Condizioni risultato.
2. Se si sta creando un processo di rapporto pianificato o un processo di alert, fare clic sulla scheda Eventi o Incidenti per impostare il tipo di filtro appropriato. Poiché un processo di rapporto o di avviso può contenere sia query di evento che query di incidente, è possibile impostare i tipi di filtro separatamente.
3. Utilizzare le caselle di controllo Risultati per abilitare una qualunque delle qualifiche per la visualizzazione seguenti:

   Limite query predefinito

   Questo valore è disponibile solo per gli alert e la pianificazione rapporto. Imposta il processo di avviso o di rapporto per utilizzare il limite di riga delle singole query. Nel caso in cui durante la creazione del processo venga selezionato un valore di risultato diverso, CA User Activity Reporting Module sostituisce i limiti di riga nelle query dei componenti.

   Limite righe

   Impostare il numero massimo di righe di evento visualizzate dalla query, a partire dagli eventi più recenti.

   Nessun limite

   Imposta la query per il recupero di tutti gli eventi che soddisfano il filtro. È possibile includere numerosi eventi, pertanto è necessario definire la query in maniera adeguata.

   Altro

Indica la presenza di altri risultati non visualizzati a causa della limitazione della riga. Il valore consente di eseguire un confronto tra gli eventi selezionati nel contesto di tutti gli eventi di quel tipo. Ad esempio, se si sceglie un limite di righe pari a 10 per la visualizzazione del visualizzatore eventi e si seleziona Mostra ulteriori elementi, gli eventi oltre il 10 vengono visualizzati come una singola voce denominata Altro contenente tutti gli eventi rimanenti. Questa impostazione è effettiva solo quando è selezionato il limite di righe.

Granularità temporale

Imposta il livello di dettaglio del campo relativo al periodo di tempo utilizzato nella visualizzazione della query.

4. Utilizzare le condizioni del risultato per effettuare una query per individuare vari tipi di condizioni di eventi raggruppati. Ad esempio, è possibile impostare la query per cercare l'ultimo evento raggruppato dopo una data selezionata, oppure un determinato numero di eventi raggruppati. Un evento raggruppato è un evento potenziato per cui sono stati impostati una funzione e un ordine di gruppo nella passaggio Creazione query.

   Le condizioni di raggruppamento utilizzano lo stesso sistema di descrizione temporale dei campi di intervallo di tempo.

5. Fare clic sulla freccia corrispondente per accedere al passaggio di progettazione della query che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, la nuova query viene visualizzata nell'Elenco query; altrimenti, verrà visualizzato il passaggio selezionato della procedura guidata.

Ulteriori informazioni:

Come creare una query (a pagina 305)
Modalità di impostazione delle condizioni risultato (a pagina 318)
Impostazione di un intervallo di ora o di data (a pagina 319)

Creazione di una visualizzazione di query

Per creare una nuova visualizzazione di query, è necessario impostare i dettagli Visualizzazione, che consentono di controllare le modalità di visualizzazione delle informazioni sugli eventi.

Per creare una visualizzazione di query

1. Aprire la procedura guidata Progettazione query.
2. Inserire il nome e il tag, se non sono già specificati, quindi proseguire con il passaggio Visualizzazione.
3. Scegliere se utilizzare un visualizzatore eventi o un grafico per la visualizzazione di query.

   Se si sceglie Visualizzatore eventi, il passaggio di visualizzazione viene completato. Le colonne degli eventi verranno visualizzate in Visualizzatore eventi nell'ordine in cui sono state posizionate nel passaggio di costruzione delle Colonne query.
4. Se si sceglie un grafico, è possibile selezionarne di diversi tipi. Se si selezionano più tipi di grafici, è possibile selezionarli uno alla volta nella visualizzazione dei rapporti. Le frecce verso l'alto e verso il basso che compaiono accanto a ogni tipo di grafico controllano l'ordine in cui i grafici appaiono nel menu Modifica visualizzazione.

   Nota: la visualizzazione Tabella è sempre disponibile, anche se non viene aggiunta durante questo passaggio.
5. Selezionare l'evento da visualizzare come asse X (orizzontale) dal menu a discesa della colonna, inserire il testo dell'etichetta (facoltativo), quindi selezionare una delle seguenti opzioni dal menu dei tipi di visualizzazione:
   - Categoria: utilizzare questa opzione per colonne con valori di testo o stringa, ad esempio source_username.
   - Lineare: utilizzare questa opzione per valori numerici, ad esempio event_count. Quando i valori sono ampiamente diffusi, è possibile utilizzare la casella di controllo Asse di accesso, che consente di avere un'asse logaritmica.
   - Data/ora: utilizzare questa opzione per visualizzare i valori temporali nella data e ora locali.
6. Ripetere il passaggio 4 utilizzando i menu Impostazioni asse Y per impostare le opzioni della colonna relativa all'asse Y (verticale), dell'etichetta e del tipo.

7. Fare clic sulla freccia appropriata per proseguire con il passaggio di progettazione della query che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, la nuova query viene visualizzata nell'Elenco query; altrimenti, verrà visualizzato il passaggio selezionato della procedura guidata.

Aggiunta di un rapporto drill-down

È possibile aggiungere uno o più rapporti drill-down alla propria query. Questo tipo di rapporti consente all'utente di fare clic su un elemento di visualizzazione query e di visualizzare un altro rapporto correlato.

Per aggiungere un rapporto drill-down

1. Aprire la procedura guidata Progettazione query.
2. Inserire il nome e il tag, se non sono già specificati, quindi proseguire con il passaggio Drill-down.
3. Fare clic su Aggiungi Drill-Down.
4. Immettere il nome oppure selezionare il rapporto da rendere disponibile come elemento drill-down.
5. Selezionare uno o più parametri disponibili su cui concentrare il rapporto drill-down e spostarli nell'elenco Parametri selezionati. I rapporti drill-down utilizzano i parametri selezionati per mantenere l'attenzione sulla query.
6. Fare clic sulla freccia appropriata per proseguire con il passaggio di progettazione della query che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, la nuova query viene visualizzata nell'Elenco query; altrimenti, verrà visualizzato il passaggio selezionato della procedura guidata.

Modifica di una query

È possibile modificare le query personalizzate esistenti, ma non quelle di sottoscrizione; tuttavia, è possibile copiare una query di sottoscrizione e modificarne poi la copia. Se si modifica una query, le modifiche apportate verranno applicate a tutti i rapporti che utilizzano tale query.

Per modificare una query

1. Fare clic sulla scheda Query e rapporti e sulla sottoscheda Query.

   Vengono visualizzati l'elenco Filtro tag query e l'Elenco query.

2. Espandere la cartella Utente nell'Elenco query e selezionare la query da modificare.

3. Fare clic su Opzioni nella parte superiore dell'elenco e selezionare Modifica.

   Appare la procedura guidata Progettazione query, popolata con le specifiche della query selezionata.

4. Apportare le modifiche desiderate, quindi fare clic su Salva.

Eliminazione di una query personalizzata

È possibile eliminare una query personalizzata, ma non è possibile eliminare le query di sottoscrizione.

Per eliminare una query

1. Selezionare la query da eliminare.

2. Fare clic su Opzioni nella parte superiore dell'elenco e selezionare Elimina.

   Viene visualizzata una finestra di dialogo di conferma.

3. Fare clic su Sì.

   La query eliminata viene rimossa dall'Elenco query.

Ulteriori informazioni

Disattivazione dell'opzione Mostra query selezionata (a pagina 326)
Modifica di una query (a pagina 325)
Esportazione e importazione delle definizioni delle query (a pagina 326)

Disattivazione dell'opzione Mostra query selezionata

È possibile impostare il proprio elenco query in modo da poter apportare modifiche senza caricare le query. Generalmente, la selezione di una query dall'elenco ne apre la visualizzazione nella finestra dei dettagli.

La disattivazione di questa modalità predefinita consente di risparmiare tempo e di selezionare una query dall'elenco e modificarla immediatamente, senza doverne attendere la visualizzazione. Ciò risulta utile in particolare se si devono modificare parecchie query e si conoscono già le modifiche da apportare.

Nota: dato che soltanto gli utenti con modalità amministratore o analista possono creare o modificare le query, essi saranno i soli che potranno disattivare l'impostazione Mostra query selezionata.

Per disattivare l'opzione Mostra query selezionata

1. Fare clic su Opzioni nella parte superiore dell'Elenco query.

   Viene visualizzato il menu Opzioni.

2. Deselezionare la casella di controllo accanto a Mostra query selezionata.

   Nessuna query selezionata dall'elenco verrà visualizzata fino a quando questa opzione non verrà nuovamente abilitata.

Esportazione e importazione delle definizioni delle query

È possibile esportare e importare i dettagli delle query personalizzate per l'utilizzo in altri server di gestione. In questo modo, è possibile trasferire correttamente query personalizzate in altri ambienti CA User Activity Reporting Module, oppure da un ambiente di prova a uno attivo.

Ulteriori informazioni

Importazione delle definizioni di query (a pagina 328)
Esportazione delle definizioni di query (a pagina 327)

Esportazione delle definizioni di query

È possibile esportare i dettagli di query create dall'utente per l'utilizzo in altri server di gestione. Il file di esportazione viene salvato in formato XML.

Per esportare i dettagli delle query

1. Fare clic sulla scheda Query e rapporti, quindi sulla sottoscheda Query.

   Viene visualizzato l'Elenco query.

2. Fare clic su Opzioni nella parte superiore dell'elenco e selezionare Esporta.

   Viene visualizzata la finestra di dialogo Esporta definizioni di query utente, in cui vengono mostrati i rapporti disponibili creati dall'utente.

3. Selezionare le query da esportare mediante il controllo pilota, quindi fare clic su Esporta.

   Viene visualizzata la finestra di dialogo di esportazione.

4. Immettere o selezionare la posizione in cui salvare i file di esportazione XML, quindi fare clic su Salva.

   I file delle query vengono salvati nella posizione selezionata, quindi viene visualizzata una finestra di dialogo di conferma.

5. Fare clic su OK, quindi selezionare Chiudi.

   La finestra di dialogo Esporta definizioni di query utente viene chiusa.

Ulteriori informazioni

Esportazione e importazione delle definizioni delle query (a pagina 326)
Importazione delle definizioni di query (a pagina 328)

Importazione delle definizioni di query

È possibile importare i file XML con le definizioni delle query da utilizzare nel server di gestione locale.

Per importare i dettagli dei rapporti

1. Fare clic sulla scheda Query e rapporti, quindi sulla sottoscheda Query.

   Viene visualizzato l'Elenco query.

2. Fare clic su Opzioni nella parte superiore dell'elenco e selezionare Importa.

   Viene visualizzata la finestra di dialogo relativa all'importazione del file.

3. Immettere o individuare la posizione in cui importare il file, quindi fare clic su OK.

   Viene visualizzata la finestra Importa risultati.

4. Fare clic su Importa altro file per ripetere il passaggio 3 oppure selezionare Chiudi.

   La finestra Importa risultati viene chiusa.

Ulteriori informazioni

Esportazione e importazione delle definizioni delle query (a pagina 326)
Esportazione delle definizioni di query (a pagina 327)

Modalità di creazione di un rapporto

È possibile creare rapporti personalizzati per il proprio ambiente, utilizzando il processo descritto in questa sezione per creare un rapporto completamente nuovo, oppure ricorrendo ad un rapporto predefinito come modello. È possibile visualizzare i rapporti personalizzati oppure impostarli come modelli di rapporto pianificati.

Esiste anche la possibilità di modificare o eliminare i rapporti personalizzati e di esportarne le informazioni. Queste attività di personalizzazione possono essere eseguite soltanto se si è effettuato l'accesso con ruolo di amministratore o analista.

La creazione di un nuovo rapporto tramite la procedura guidata Progettazione rapporto si articola nei passaggi seguenti:

1. Apertura della procedura guidata Progettazione rapporto.
2. Aggiunta di dettagli al rapporto: assegnazione di un nome e di tag di categoria al nuovo rapporto.
3. Strutturazione di un layout per il rapporto: selezione delle query da includere nel rapporto e della relativa modalità di visualizzazione.

Apertura della procedura guidata Progettazione rapporto

Per creare un rapporto personalizzato completamente nuovo o uno basato su un rapporto esistente, è necessario aprire la procedura guidata Progettazione rapporto.

Per aprire la procedura guidata Progettazione rapporto

1. Fare clic sulla scheda Query e rapporti, quindi sulla sottoscheda Rapporti.

   Viene visualizzato l'Elenco rapporti.

2. Fare clic su Opzioni, quindi selezionare Nuovo o Copia.

   Viene visualizzata la procedura guidata Progettazione report.

   Mentre si utilizza la procedura guidata:

   - Fare clic su Salva per salvare senza chiudere la procedura.
   - Fare clic su Salva e chiudi per salvare il rapporto e chiudere la procedura.
   - Fare clic su Ripristina per ripristinare la visualizzazione della procedura con le ultime impostazioni salvate.

Aggiunta di dettagli al rapporto

È possibile creare un nuovo rapporto oppure da una copia di un rapporto esistente. Quando si crea un rapporto, gli si assegna un nome e si aggiungono le eventuali sottoscrizioni o tag personalizzati che si desidera associare al rapporto stesso.

Per aggiungere dettagli al rapporto

1. Aprire la procedura guidata Progettazione rapporto.
2. Assegnare un nome al rapporto. È anche possibile immettere informazioni descrittive facoltative da usare come riferimento.
3. Selezionare il tipo di connessione desiderato. Il valore UARM predefinito viene visualizzato nell'elenco a discesa assieme ai nomi delle connessioni ODBC impostate nell'area Servizio di rapporto.

   UARM predefinito

   Indirizza il rapporto ai database di eventi interni e di incidenti.

   Connessioni ODBC

   Indirizza il rapporto a una tabella ODBC esterna selezionata. Per completare un rapporto, è necessario disporre di query ODBC personalizzate indirizzate verso il database selezionato.

4. Selezionare uno o più tag da associare al rapporto tramite il Controllo pilota tag.
5. (Facoltativo) Per aggiungere un tag di categoria personalizzato, inserire un nome tag nel campo di immissione Aggiungi tag personalizzato e fare clic su Aggiungi tag.

   Il tag personalizzato appare come nell'Elenco tag selezionati.
6. (Facoltativo) Per aggiungere uno o più tag nidificati, selezionare un tag oppure digitare il nome del tag padre seguito da una barra rovesciata, quindi digitare il nome del tag figlio. Quindi selezionare Aggiungi tag. Ad esempio, è possibile digitare: "Normative\Standard del settore". È possibile aggiungere ulteriori tag, mantenendo il formato a\b\c e così via.

   Nota: se si elimina uno dei tag nidificati personalizzati, verranno eliminati anche tutti i tag in cui è nidificato, compreso il tag padre. Se si nidifica un tag personalizzato all'interno di un tag di sottoscrizione e quindi lo si elimina, verranno eliminati solo i tag personalizzati.

   Una volta completato il processo, il nuovo tag viene visualizzato nell'elenco, con i tag personalizzati nidificati visibili quando si espande il tag padre.
7. Proseguire con il passaggio Layout o fare clic su Salva e chiudi se è già stata selezionata almeno una query.

Progettazione del layout rapporto

È possibile progettare una struttura di rapporto specificando la dimensione della griglia, quindi selezionando le query da visualizzare in ciascuna sezione della griglia. Un rapporto può contenere query CA User Activity Reporting Module interne o query indirizzate a un database ODBC esterno, ma non entrambe.

Per progettare un layout rapporto

1. Aprire la procedura guidata Progettazione rapporto. Se il rapporto è nuovo, inserire un nome, selezionare un tag e proseguire con il passaggio Layout.
2. Selezionare o immettere il numero di righe e colonne che si desidera visualizzare nel rapporto mediante le aree Righe griglia e Colonne del riquadro Layout rapporto. Tali impostazioni consentono di controllare il numero di aree di visualizzazione di query contenute nel rapporto. È possibile includere fino a un massimo di 10 righe e/o colonne.

   Il numero appropriato di righe, colonne e di query corrispondenti viene visualizzato nel riquadro del layout dei rapporto.

   Nota: è possibile utilizzare le frecce situate nella parte inferiore e destra delle singole aree di visualizzazione delle query per espanderle o comprimerle orizzontalmente o verticalmente.
3. (Facoltativo) Inserire o selezionare la dimensione minima dei pixel per le aree di visualizzazione delle query nelle aree Larghezza minima e Altezza minima.
4. Trascinare la query da visualizzare in ciascun'area di visualizzazione dall'elenco query nell'area corrispondente del layout di rapporto:
   - Se si crea un rapporto standard, l'elenco conterrà query di eventi e di incidenti.
   - Se si crea un rapporto ODBC, le query indirizzate verso il database selezionato nella prima schermata della procedura guidata verranno visualizzate nell'elenco.
5. (Facoltativo) Fare clic su Modifica nella parte superiore di ciascuna area di visualizzazione delle query per modificare la query in questione o creare una nuova query personalizzata.
6. Fare clic su Salva e chiudi.

   La procedura guidata Progettazione rapporto viene chiusa. Il nuovo rapporto verrà visualizzato nell'Elenco rapporti sotto la cartella Utente.

Ulteriori informazioni:

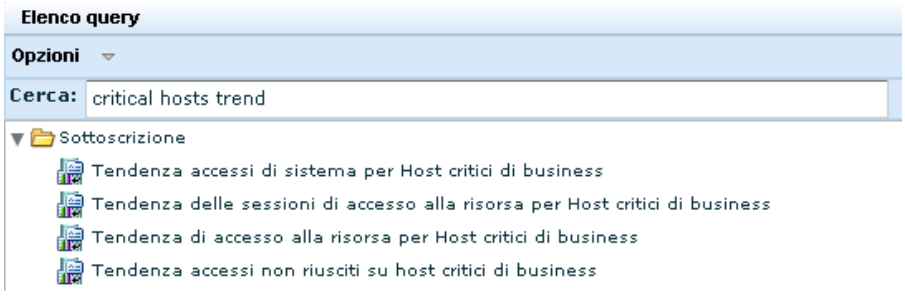
Aggiunta di dettagli al rapporto (a pagina 330)

Esempio: creazione di un rapporto da query esistenti

È possibile creare rapporti personalizzati composti da query predefinite e adattarli alle proprie specifiche.

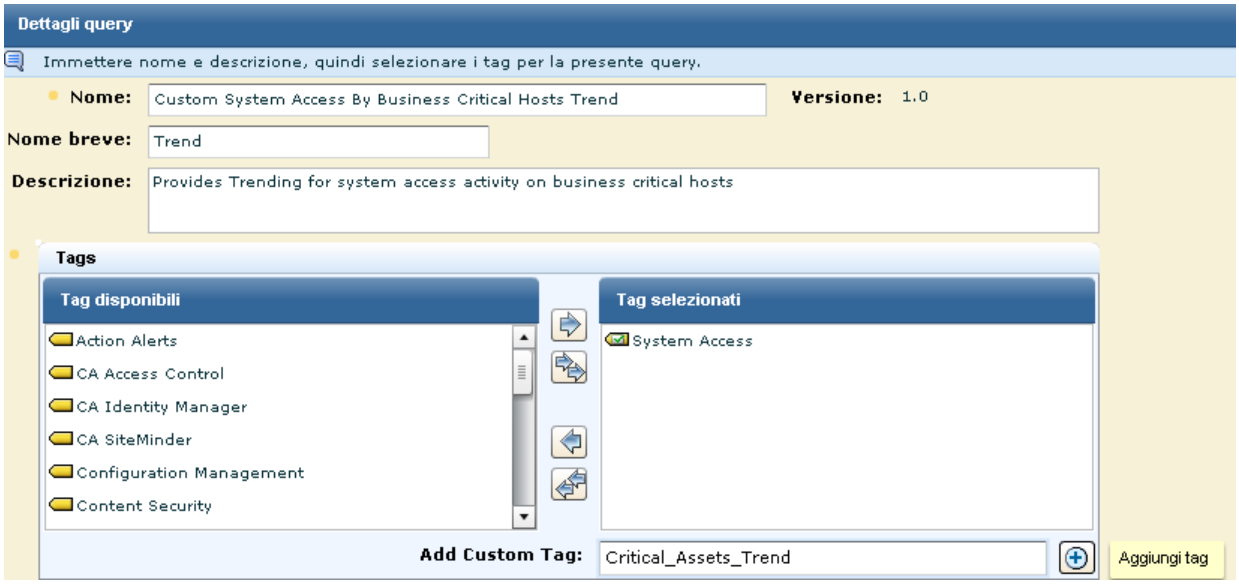
Per creare un rapporto da query esistenti

1. Identificare le query da includere nel rapporto personalizzato.
   a. Fare clic sulla scheda Query e rapporti e sulla sottoscheda Query, se non viene visualizzata.
   b. Immettere una parola o una frase chiave nel campo Cerca per visualizzare le query con il contenuto dal quale si desidera apportare una selezione. Ad esempio, digitare Tendenza host critici.
   c. Annotare i nomi delle query da includere nel rapporto personalizzato. Ad esempio, è possibile definire un rapporto delle tendenze associate agli host critici di business osservando quelle elencate nell'illustrazione seguente, dove sono riportate quelle per l'accesso al sistema, l'accesso alle risorse e le creazioni di account.



2. Per la prima query da includere nel rapporto, creare una copia e aggiungere un tag personalizzato.
   a. Selezionare una query, quindi fare clic su Copia dall'elenco a discesa Opzioni.
   b. Rinominare la query e inserire un tag personalizzato da aggiungere. Ad esempio, rinominare Copia di Tendenza accessi di sistema per host critici di business in Tendenza accessi di sistema per host critici di business personalizzata.

c. Aggiungere un tag personalizzato. Ad esempio, inserire Critical_Assets_Trend e fare clic su Aggiungi tag.

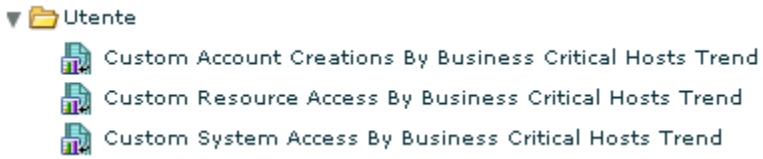


d. Fare clic sul pulsante Sposta per spostare il tag preselezionato nell'area Tag disponibili. Ad esempio, spostare Accesso al sistema. L'unico tag selezionato è quello aggiunto.

e. Fare clic su Salva e chiudi.

3. Per le altre query da includere nel rapporto, creare una copia e selezionare il tag personalizzato creato.
   a. Selezionare una query, quindi fare clic su Copia dall'elenco a discesa Opzioni.
   b. Rinominare la query e selezionare il nuovo tag personalizzato. Ad esempio, rinominare Copia di Tendenza accesso alla risorsa per host critici di business in Tendenza accesso alla risorsa per host critici di business personalizzata, spostare Critical_Assets_Trend nell'elenco Tag selezionati e rimuovere il tag preselezionato.
   c. Fare clic su Salva e chiudi.

   Le query copiate vengono visualizzate in Utente:

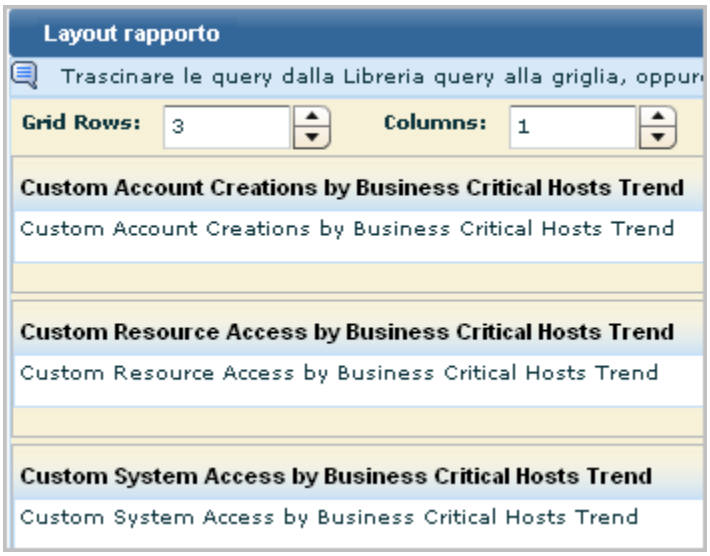
   

4. se le query sono associate a elenchi con chiave, definire i valori per quell'elenco con chiave.
5. Avviare il processo di creazione del rapporto come segue:
   a. Fare clic sulla scheda Query e rapporti, quindi sulla sottoscheda Query.
   b. Selezionare Nuovo dall'elenco a discesa Opzioni nell'Elenco rapporti.

      Viene visualizzata la procedura guidata Progettazione report.

      Aggiungere il tag personalizzato, Critical_Assets_Trend.

6. Progettare il layout del rapporto.



7. Fare clic su Salva e chiudi.
8. Pianificare il rapporto basato sul tag personalizzato creato dall'utente.
9. Visualizzare il rapporto.

Nota: è consigliabile esaminare tutti i rapporti nuovi per verificare che forniscano le informazioni desiderate nel miglior modo possibile.

Esempio: impostazione della federazione e dei rapporti federati

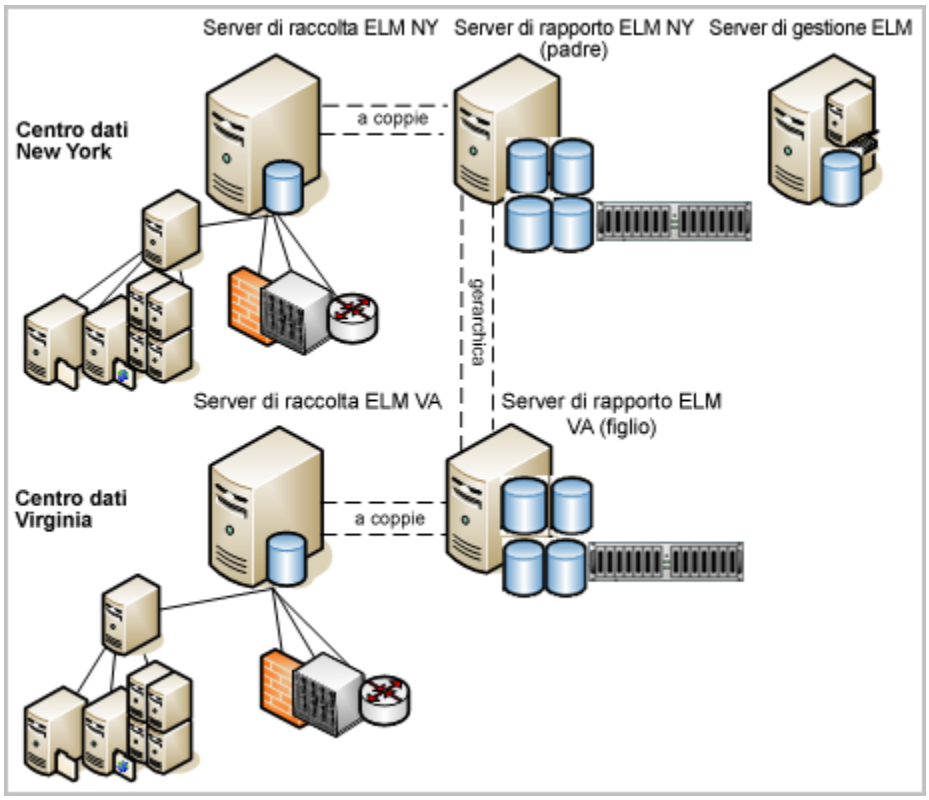
È possibile raccogliere i log da centri dati di grandi dimensioni con posizioni geografiche diverse ed impostare i rapporti in modo tale che i dati distribuiti siano inviati da un solo centro dati.

Ad esempio, si dispone di due centri dati di grandi dimensioni locati a New York e in Virginia, con New York come sede centrale. Ogni centro dati dispone di un server di raccolta che raccoglie ed elabora i log eventi in arrivo e li invia al proprio server di rapporto. Il server di rapporto gestisce query, avvisi e rapporti. La maggior parte di query, avvisi e rapporti si concentra sui dati degli eventi raccolti tramite gli agenti; il consolidamento dei dati provenienti da queste origini evento richiede la federazione tra i server di rapporto e quelli di raccolta.

Alcune query, avvisi e rapporti si concentrano sugli eventi di automonitoraggio generati dai server CA User Activity Reporting Module; il consolidamento di questo tipo di dati richiede l'inclusione del server di gestione nella federazione. Se non si desidera eseguire il consolidamento dei dati degli eventi di automonitoraggio, è possibile escludere il server di gestione dalla federazione. Gli eventi di automonitoraggio provenienti da questo server possono essere monitorati tramite rapporti locali non federati. Per una maggiore semplicità, il server di gestione viene escluso dalla federazione. Per includere il server, creare una federazione a coppie tra i server di rapporto ELM NY e server di gestione ELM.

I nomi dei server sono i seguenti:

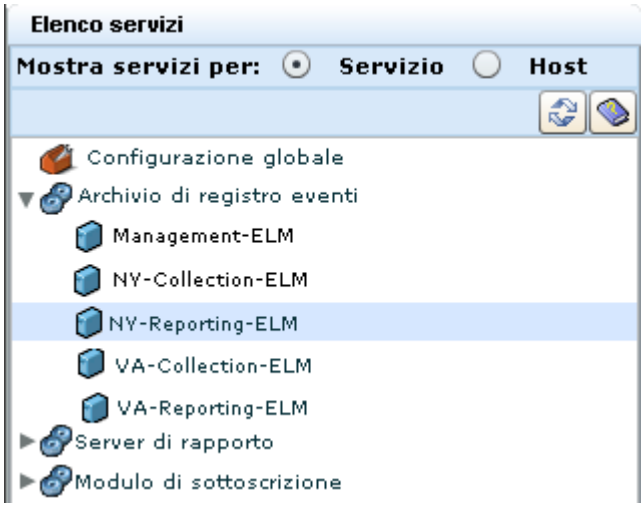
- Server di gestione ELM
- Server di raccolta ELM NY
- Server di rapporto ELM NY
- Server di raccolta ELM VA
- Server di rapporto ELM VA



L'amministratore di New York desidera ricevere tutti i rapporti e gli avvisi eseguiti dalla sede di New York per includere i dati provenienti dalla sede di Virginia, ma desidera che i rapporti e gli avvisi eseguiti dalla sede in Virginia includano solamente i dati raccolti a livello locale.

L'esempio riportato di seguito mostra la modalità per la creazione di una federazione tra i server e per la configurazione della creazione dei rapporti per soddisfare i criteri dello scenario. Le procedure per la configurazione dell'archiviazione automatica non sono incluse nell'esempio, però tale funzione dovrebbe essere configurata in tutte le architetture dai grandi volumi.

1. Accedere a CA User Activity Reporting Module con le credenziali di amministratore.
2. Fare clic sulla scheda Amministrazione e selezionare la sottoscheda Servizi.
3. Attenersi alla seguente procedura per creare una federazione gerarchica, con il server di rapporto ELM NY come padre e il server di rapporto ELM VA come figlio:
   a. Espandere il deposito eventi di log, quindi selezionare il nome del server che si desidera impostare come padre nella federazione gerarchica, in questo caso, il server di rapporto ELM NY.



   b. Selezionare il server di rapporto ELM VA dall'elenco dei server figlio della federazione disponibili, quindi spostarlo nell'elenco dei server selezionati.

4. Attenersi alla seguente procedura per creare una federazione a coppie tra i server di rapporto ELM NY e il server di raccolta ELM NY, in cui ciascuno è figlio dell'altro.
   a. Selezionare il server di rapporto ELM NY dall'elenco del deposito eventi di log.
   b. Selezionare il server di raccolta ELM NY dall'elenco dei server figlio della federazione disponibili, quindi spostarlo nell'elenco dei server selezionati.
   c. Selezionare il server di raccolta ELM NY dall'elenco del deposito eventi di log.
   d. Selezionare il server di rapporto ELM NY dall'elenco dei server figlio della federazione disponibili, quindi spostarlo nell'elenco dei server selezionati.
5. Attenersi alla seguente procedura per creare una federazione a coppie tra i server di rapporto ELM VA e il server di raccolta ELM VA, in cui ciascuno è figlio dell'altro.
   a. Selezionare il server di rapporto ELM VA dall'elenco del deposito eventi di log.
   b. Selezionare il server di raccolta ELM VA dall'elenco dei server figlio della federazione disponibili, quindi spostarlo nell'elenco dei server selezionati.
   c. Selezionare il server di raccolta ELM VA dall'elenco del deposito eventi di log.
   d. Selezionare il server di rapporto ELM VA dall'elenco dei server figlio della federazione disponibili, quindi spostarlo nell'elenco dei server selezionati.
6. Attenersi alla seguente procedura per configurare le impostazioni globali del server di rapporto e degli override locali per il server di rapporto ELM VA. I server geograficamente distanti utilizzano spesso server di posta elettronica diversi.
   a. Selezionare Alerting Service (Servizio Avvisi) da Elenco servizi.
   b. Configurare le impostazioni globali o locali necessarie per le opzioni del server di posta elettronica dal nodo del server di rapporto ELM NY.
   c. Se si desidera inviare i rapporti tramite posta elettronica, selezionare Server di rapporto e quindi il nodo del server di rapporto ELM NY.
   d. Impostare le opzioni di formato PDF globali o locali o le opzioni di rapporto relative alla memorizzazione di rapporti e avvisi.

7. Per ciascun rapporto pianificato la cui esecuzione è pianificata dal server di rapporto ELM NY, eseguire le seguenti operazioni:
   a. Fare clic sulla scheda Rapporti pianificati e sulla scheda Pianificazione rapporto.
   b. Fare clic su Pianifica rapporto.
   c. Selezionare il rapporto da pianificare e completare i passaggi 2, 3, 4 e 5 secondo necessità.
   d. Fare clic sul passaggio Selezione server, scegliere Server di rapporto ELM NY dall'elenco dei server disponibili e spostarlo nell'elenco dei server selezionati. Dopodichè, accettare l'impostazione predefinita, Sì, per le query federate.
   e. Fare clic su Salva, quindi su Chiudi.

I rapporti includono i dati ottenuti dal server di rapporto ELM NY e dal relativo peer, dal server di raccolta ELM NY e dal figlio corrispondente, dal server di rapporto ELM VA, e dal peer figlio corrispondente, ovvero il server di raccolta ELM VA.

Nota: una query federata eseguita dal server di rapporto ELM VA include i dati del server di rapporto ELM VA e del relativo peer, ovvero il server di raccolta ELM VA. Non includono i dati provenienti dal server di rapporto ELM NY, in quanto tale server corrisponde all'elemento padre della federazione gerarchica.

Modifica di un rapporto

È possibile modificare un rapporto personalizzato.

Nota: l'opzione Mostra rapporto selezionato può essere disabilitata quando si modificano più rapporti. Questo consente di selezionare e modificare rapporti senza doverne attendere la visualizzazione del riquadro dei dettagli.

Per modificare un rapporto

1. Selezionare il rapporto che si desidera modificare dall'Elenco rapporti.
2. Fare clic su Opzioni nella parte superiore dell'elenco e selezionare Modifica.

   Viene visualizzata la procedura guidata Progettazione rapporto, popolata con le specifiche del rapporto selezionato.
3. Apportare le modifiche desiderate, quindi fare clic su Salva e chiudi.

   Il rapporto modificato viene visualizzato nell'Elenco rapporti sotto la cartella Utente.

Eliminazione di un rapporto personalizzato

È possibile eliminare un rapporto personalizzato, ma non i rapporti di sottoscrizione.

Per eliminare un rapporto personalizzato

1. Selezionare il rapporto personalizzato che si desidera eliminare dall'Elenco rapporti.
2. Fare clic su Opzioni nella parte superiore dell'elenco e selezionare Elimina.

   Viene visualizzata una finestra di dialogo di conferma.
3. Fare clic su Sì.

   Il rapporto eliminato viene rimosso dall'Elenco rapporti.

Ulteriori informazioni

Modalità di creazione di un rapporto (a pagina 329)
Modifica di un rapporto (a pagina 342)

Esempio: eliminazione dei rapporti giornalieri con più di 30 giorni

È possibile implementare i criteri relativi alla memorizzazione dei rapporti tramite la configurazione globale dei server di rapporto. Si possono impostare criteri di memorizzazione diversi per ogni ricorrenza dei rapporti pianificati, ovvero:

- Memorizzazione rapporti singoli
- Memorizzazione rapporti giornalieri
- Memorizzazione rapporti settimanali
- Memorizzazione rapporti mensili
- Memorizzazione rapporti annuali

Occorre modificare l'impostazione predefinita Non eseguire mai per l'utility Memorizzazione rapporti in una frequenza. Assicurarsi che la frequenza con cui vengono impostate le esecuzioni dell'utility sia abbastanza alta da eseguire le rimozioni secondo la frequenza configurata. Ad esempio, per eliminare i rapporti giornalieri un giorno dopo l'esecuzione e si pianifica che tali rapporti debbano essere eseguiti alle 6.00 e alle 18.00, l'utility di memorizzazione rapporti verrà impostata in modo da avviarsi come minimo ogni 12 ore.

Esempio: eliminazione dei rapporti giornalieri con più di 30 giorni

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.

   L'Elenco servizi mostra i singoli servizi.

2. Fare clic su Server di rapporto.

   Viene visualizzata la Configurazione di servizio globale: Server di rapporto.

3. Utilizzare le seguenti linee guida per completare la configurazione:
   - Per automatizzare l'eliminazione dei rapporti giornalieri 30 giorni dopo la loro generazione, impostare la memorizzazione di tali rapporti per essere rimossa dopo trenta giorni.
   - Assicurarsi di impostare l'utility Memorizzazione rapporti in modo che si avvii secondo il numero specificato di ore, giorni o settimane.

4. Fare clic su Salva.

Esportazione delle definizioni dei rapporti

È possibile esportare i dettagli dei file creati dall'utente per utilizzarli in altri server di gestione. Il file di esportazione viene salvato in formato XML. Una definizione di rapporto esportata include le definizioni per tutte le query di quel rapporto.

Per esportare i dettagli dei rapporti

1. Fare clic sulla scheda Query e rapporti, quindi sulla sottoscheda Query.

   Viene visualizzato l'elenco dei rapporti.

2. Fare clic su Opzioni nella parte superiore dell'elenco e selezionare Esporta.

   Viene visualizzata la finestra di dialogo Esporta definizioni report utente, in cui vengono mostrati i rapporti creati dall'utente disponibili.

3. Selezionare i rapporti da esportare mediante il comando principale, quindi fare clic su Esporta.

   Viene visualizzata la finestra di dialogo di esportazione.

4. Immettere o selezionare la posizione in cui salvare i file di esportazione XML, quindi fare clic su Salva.

   I file dei rapporti vengono salvati nella posizione selezionata, quindi viene visualizzata una finestra di dialogo.

5. Fare clic su OK, quindi selezionare Chiudi.

   La finestra di dialogo Esporta definizioni report utente viene chiusa.

Ulteriori informazioni

Importazione delle definizioni dei rapporti (a pagina 346)

Importazione delle definizioni dei rapporti

È possibile importare i file XML con le definizioni dei rapporti da utilizzare nel server locale di gestione.

Per importare i dettagli dei rapporti

1. Fare clic sulla scheda Query e rapporti, quindi sulla sottoscheda Query.

   Viene visualizzato l'elenco dei rapporti.

2. Fare clic su Opzioni nella parte superiore dell'elenco e selezionare Importa.

   Viene visualizzata la finestra di dialogo Importa file.

3. Immettere o individuare la posizione in cui importare il file, quindi fare clic su OK.

   Viene visualizzata la finestra Importa risultati.

4. Fare clic su Importa altro file per ripetere il passaggio 3 oppure selezionare Chiudi.

   Viene chiusa la finestra Importa rapporto utente e definizioni query.

Ulteriori informazioni

Esportazione delle definizioni dei rapporti (a pagina 345)

Preparazione all'utilizzo di rapporti dotati di elenchi con chiave

Tutti rapporti vengono creati a partire da una o più query. Alcune query utilizzate nei rapporti predefiniti sono progettate in modo tale da selezionare tutti valori di una determinata tabella, in cui un determinato campo di attributo contiene un valore utilizzato come criterio per compilare l'elenco dei valori principali. Ad esempio, una tabella di risorse è dotata del campo IsCritical. Una query che selezioni tutti nomi di risorsa dalla tabella delle risorse in cui IsCritical è uguale a Yes selezionerà solo i nomi delle risorse critiche. Questi nomi possono essere restituiti a CA User Activity Reporting Module per aggiornare i valori della chiave Critical_Assets.

La preparazione per l'utilizzo dei rapporti predefiniti con gli elenchi con chiave si basa sulle seguenti operazioni:

- (Facoltativo) Consentire l'importazione dei valori dinamici, a patto di utilizzare CA IT PAM.
- Creare elenchi con chiave per le chiavi predefinite prive di valori predefiniti.
- Creare elenchi con chiave per le chiavi predefinite dotate di valori predefiniti.
- Conservare gli elenchi con chiave utilizzati nei rapporti predefiniti che si desidera utilizzare. Aggiornare ogni elenco con chiave con i valori attuali.

Inoltre, è possibile aggiungere nuove chiavi per i rapporti personalizzati che utilizzano elenchi con chiave e quindi aggiungere valori per ogni nuova chiave. Infine, è possibile aggiungere valori alle chiavi Business_Critical_Sources ed ELM_System_Lognames per le query su richiesta progettate dall'utente.

Abilitare l'importazione di valori dinamici

Le procedure necessarie per abilitare l'importazione dei valori dinamici si applicano solo agli utenti di CA IT PAM.

Se si utilizza CA IT PAM e si dispone di tabelle o fogli di calcolo esistenti in cui si conservano gli elenchi di file, database, host, utenti e così via, è possibile sfruttare questi dati. È possibile creare un processo per leggere la tabella o il file, selezionare i valori pertinenti alla chiave e restituire tali valori all'elenco dei valori di CA User Activity Reporting Module per tale chiave.

Per importare valori dinamici

1. Creare in CA IT PAM un processo per ogni elenco di valori chiave da generare su richiesta.

   Nota: se un qualsiasi processo legge una tabella di database, installare un agente CA IT PAM sul server con il database di SQL Server 2005.

2. Configurare l'integrazione di CA IT PAM per i valori dinamici in CA User Activity Reporting Module.

Ulteriori informazioni:

Creare un processo CA IT PAM per generare un elenco di valori (a pagina 349)
Configurare l'integrazione di CA IT PAM per i valori dinamici (a pagina 350)

Informazioni sui processi di valori dinamici

Un processo di valori dinamici è un processo CA IT PAM che è possibile richiamare per compilare o aggiornare l'elenco dei valori di una chiave selezionata, utilizzata in rapporti e avvisi. Si presume che siano già memorizzati gli elenchi master di file, database, host, utenti e così via che compongono l'ambiente di lavoro e che questi elenchi master contengano attributi che permettono di eseguire una query per set di valori di interesse. Se si utilizza CA IT PAM, è possibile creare processi da richiamare per eseguire le query che restituiscono a CA User Activity Reporting Module i dati da utilizzare come valori chiave nei rapporti e negli avvisi basati sulle chiavi. La capacità di creare un elenco di valori in maniera dinamica è utile per tenere aggiornati gli elenchi di chiavi volatili con i valori attuali.

Creare un processo CA IT PAM per generare un elenco di valori

In CA IT PAM è possibile creare un processo per ogni elenco di valori principali che si desidera generare su richiesta. Consultare la documentazione di CA IT PAM per ulteriori informazioni sulla creazione del processo. Ogni processo deve soddisfare i requisiti di CA User Activity Reporting Module di InputKey, i parametri di processo locali ValueList e FaultString e gli operatori di calcolo Success e Failure.

Attenersi alle seguenti indicazioni:

- Il processo deve accettare la chiave selezionata come InputKey.
- Il processo deve definire i due seguenti parametri di processo locali:
  - ValueList recupera l'elenco dei valori
  - FaultString recupera la stringa di errore

  Nota: CA User Activity Reporting Module necessita di questi precisi nomi di parametro da utilizzare come parametri di interfaccia di output.
- Il processo deve contenere i due seguenti operatori di calcolo:
  - Operatore di calcolo Success: Process.ValueList =<variabile contenente l'elenco dei valori separati da virgola>
  - Operatore di calcolo Failure: Process.FaultString =<variabile contenente il messaggio di errore>

Se si crea uno script, tenere in considerazione le seguenti linee guida aggiuntive:

- Se lo script seleziona le colonne di una tabella di database, sul server in cui è installato SQL Server 2005 deve essere presente un agente di IT PAM. I server SQL devono essere elencati nel proprio dominio in Tutti i touchpoint. Il server SQL contenente i dati principali deve visualizzare il nome di agente per il server SQL.
- Lo script inline deve eseguire l'utilità sqlcmd per ottenere l'elenco desiderato.

Ulteriori informazioni:

Configurare l'integrazione di CA IT PAM per i valori dinamici (a pagina 350)

Configurare l'integrazione di CA IT PAM per i valori dinamici

È possibile configurare l'integrazione di CA IT PAM in modo da sfruttare uno o entrambi i seguenti tipi di processi di CA IT PAM.

- Processi di output di evento/avviso: processo che richiama l'elaborazione di un sistema di terze parti, ad esempio un prodotto help desk
- Processo di valori dinamici: processo che accetta una chiave di input e restituisce i valori attuali ad essa relativi sottoforma di file di elenco separato da virgole (*.csv)

La configurazione di uno di questi scopi presume la possibilità di avviare e accedere a CA IT PAM. Raccogliere i seguenti valori:

- Nome host completo o indirizzo IP del server di CA IT PAM
- Porta (la predefinita è 8080)
- Nome utente e password utilizzati da CA User Activity Reporting Module per accedere a CA IT PAM

La configurazione di CA IT PAM per i valori dinamici consente di importare l'elenco dei valori generati dinamicamente dal processo dei valori dinamici configurato. L'importazione viene eseguita impostando o aggiornando i valori con chiave utilizzati in alcuni tipi di rapporto ed avvisi.

La seguente procedura riguarda sia le impostazioni comuni che quelle specifiche dei valori dinamici.

Per configurare l'integrazione di CA IT PAM per il processo di valori dinamici

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
2. Fare clic su Server di rapporto.

   Viene visualizzata la Configurazione di servizio globale: Server di rapporto.
3. Scorrere fino all'area IT PAM.
4. Eseguire le seguenti operazioni per abilitare l'accesso a CA IT PAM:
   a. Inserire il nome host completo del server su cui è installato IT PAM.
   b. Accettare la porta predefinita, ossia la numero 8080.
   c. Inserire credenziali di accesso valide per IT PAM
5. Inserire un percorso di processo nel campo Processo valori dinamici.

   Questo percorso di processo diventerà predefinito al momento di importare i valori dinamici.
6. Fare clic su Salva.

   Verrà visualizzato il messaggio di conferma: Modifiche configurazione salvate con successo.

Approcci alla manutenzione degli elenchi con chiave

Gli elenchi con chiave vengono utilizzati in alcuni rapporti e query predefinite contrassegnati come adatti agli avvisi. Se si prevede di utilizzare questi rapporti o di creare avvisi che utilizzano queste query, è possibile utilizzare una qualsiasi combinazione dei seguenti approcci per gestire gli elenchi con chiave.

- È possibile aggiungere valori chiave direttamente per ogni chiave selezionata. È inoltre possibile selezionare qualsiasi valore di chiave per poi modificarlo o eliminarlo.
- È possibile importare i valori chiave memorizzati in un elenco CSV. In alternativa, è possibile esportare l'elenco corrente dei valori come file CSV, aggiornare il file ed importarlo per compilare l'elenco dei valori.
- È possibile eseguire un processo CA IT PAM in grado di generare un elenco corrente in maniera dinamica e di restituire i valori sottoforma di file CSV utile per compilare l'elenco dei valori.

Se si prevede di creare rapporti personalizzati che utilizzano un elenco con chiave, è possibile aggiungere una chiave personalizzata e quindi aggiungere o importare i relativi valori.

È possibile identificare l'elenco o gli elenchi con chiave utilizzati in una query ed aggiornare l'elenco prima di pianificare un rapporto o un avviso che includa tale query.

Ulteriori informazioni:

Aggiornare manualmente un elenco con chiave (a pagina 354)
Aggiornare l'elenco con chiave con esporta/importa: (a pagina 355)
Esempio: aggiornare un elenco con chiave usando un file CSV (a pagina 357)
Utilizzo delle query con il tag Avviso (a pagina 367)

Creazione di un elenco con chiave

Gli elenchi con chiave consentono di creare un gruppo e assegnarvi valori. È quindi possibile eseguire una query sul nome del gruppo e qualsiasi valore presente nel gruppo restituirà un risultato positivo. È possibile assegnare i valori individualmente, oppure importarli da un file .csv. È possibile creare elenchi con chiave personalizzati, oppure aggiungere valori agli elenchi predefiniti.

Ad esempio, alcune query per i rapporti di concessione privilegi ricercano un valore chiave denominato "Privileged_Groups". Quando una query include questo valore, restituisce tutte le righe in cui tale campo contiene qualsiasi valore specificato nel gruppo.

Per creare un elenco con chiave

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria, infine sulla cartella Elenco con chiave.
2. Fare clic su Nuovo per creare un nuovo elenco, oppure selezionare l'elenco al quale si desidera aggiungere valori.

   Nel riquadro destro vengono visualizzati i dettagli relativi all'elenco con chiave.
3. Digitare un nome e una descrizione per l'elenco con chiave e selezionare un tipo.
4. Immettere il processo di valori dinamici IT PAM che genera i valori per la chiave selezionata.

   Nota: il processo di valori dinamici IT PAM aggiorna solo l'elenco utenti della tabella Valori elenco con chiave. L'elenco utenti viene sovrascritto periodicamente con i valori più recenti.
5. (Facoltativo) Per verificare la validità del processo dei valori dinamici IT PAM immesso, fare clic sull'icona di test.

   Se la connessione viene eseguita correttamente, viene visualizzato un messaggio di conferma.
6. Se si desidera importare valori, passare al punto 10. Se si desidera aggiungere valori singolarmente, passare al punto 7.
7. Fare clic su Aggiungi nella parte superiore della tabella Valori elenco con chiave.

   Nella colonna Utente viene visualizzata una riga evidenziata.
8. Fare clic sulla riga e digitare un valore.
9. Ripetere i passaggi 6-7 per aggiungere ulteriori valori.

10. Fare clic su Importa nella parte superiore dell'area Dettagli elenco con chiave, individuare il file contenente i valori da importare e fare clic su OK.

    I valori vengono visualizzati nell'area corrispondente.

    Nota: è possibile importare solo file CSV che non contengano caratteri speciali.

11. Dopo aver aggiunto tutti i valori desiderati, fare clic su OK.

    Il nuovo elenco viene visualizzato nella cartella Utente della cartella Elenchi con chiave.

Aggiornare manualmente un elenco con chiave

I valori di un elenco con chiave possono essere aggiornati in diversi modi. Uno di essi consiste nell'aggiungere, modificare ed eliminare manualmente i valori.

Per aggiornare manualmente un elenco con chiave

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria, infine sulla cartella Elenco con chiave.
2. Espandere la cartella Elenco con chiave e selezionare l'elenco con chiave che si desidera aggiornare.
3. Per aggiungere un valore all'elenco con chiave:
   a. Selezionare la chiave a cui si desidera aggiungere un valore.
   b. Fare clic su Aggiungi valore.
   c. Immettere il nome del valore nel campo Nome e fare clic su OK.

      Il valore aggiunto verrà visualizzato nell'elenco Valori per la chiave selezionata.

   d. Ripetere questa procedura per aggiungere altri valori.
4. Per eliminare un valore da un elenco con chiave:
   a. Selezionare la chiave con un valore non necessario.
   b. Selezionare il valore da eliminare e fare clic su Rimuovi valore.

      Viene visualizzato un messaggio di conferma.

   c. Fare clic su OK.

      Il valore verrà eliminato dall'elenco Valori della chiave selezionata.

   d. Ripetere questa procedura per eliminare altri valori.

5. Per modificare un valore nell'elenco con chiave:
   a. Selezionare la chiave con il valore da modificare.
   b. Selezionare il valore da modificare e fare clic su Modifica valore.
   c. Modificare la voce nel campo Nome e fare clic su OK.

      Il valore verrà visualizzato con il nome modificato nell'elenco Valori della chiave selezionata.
   d. Ripetere questa procedura per modificare altri valori.
6. Fare clic su Salva.

   I valori delle chiavi selezionate verranno aggiornati.

Aggiornare l'elenco con chiave con esporta/importa:

Se si memorizzano i valori corrispondenti ad una chiave in un foglio di calcolo di Excel, è possibile salvare il foglio di calcolo come elenco di valori separati da virgole (*.csv) e compilare l'elenco con chiave per i valori selezionati eseguendo un'importazione.

I valori dell'elenco con chiave memorizzati in un file CSV possono essere aggiornati nei seguenti modi:

- Se il file CSV contiene i valori correnti per una data chiave e se l'elenco dei valori visualizzato non è aggiornato, è possibile importare i valori direttamente dal file CSV.
- Per creare un file CSV o per aggiornarne uno che contiene valori obsoleti, utilizzare una sequenza di operazioni di esportazione, modifica e importazione.

Per aggiornare un elenco con chiave mediante importazione o esportazione

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria, infine sulla cartella Elenco con chiave.
2. Espandere la cartella Elenco con chiave e selezionare l'elenco con chiave che si desidera aggiornare.

3. Per aggiornare i valori di una chiave selezionata a partire da un file CSV che contiene i valori correnti:
   a. Selezionare la chiave nell'elenco Valori chiave da aggiornare.
   b. Fare clic su Importa valori, nella barra degli strumenti dell'elenco Valori.

      Verrà visualizzata la finestra di dialogo Importa file.
   c. Fare clic su Sfoglia e accedere al percorso in cui è salvato il file CSV contenente i valori per la chiave selezionata.
   d. Selezionare il file da importare e fare clic su Apri, quindi fare clic su OK.

   L'elenco Valori verrà aggiornato con i valori del file CSV.
4. Per aggiornare i valori di una chiave selezionata se il file CSV non esiste o non è aggiornato:
   a. Selezionare la chiave nell'elenco Valori chiave da aggiornare.
   b. Nella barra degli strumenti Valori, fare clic su Esporta valori, accedere al percorso nel quale si desidera salvare il file CSV e fare clic su Salva.

      Verrà visualizzato un messaggio di conferma dell'operazione.
   c. Fare clic su OK.
   d. Accedere al percorso del file esportato, aprire il foglio di calcolo e modificare o eliminare le colonne esistenti come necessario. Scorrere fino a visualizzare l'ultima colonna ed aggiungere le nuove voci. Salvare quindi il file in formato CSV.
   e. Selezionare la stessa chiave e fare clic su Importa valori.
   f. Fare clic su Sfoglia, selezionare il file salvato e fare clic su Apri.
   g. Fare clic su OK.

   Il file viene caricato. È possibile scorrere fino alla parte inferiore dell'elenco Valori per confermare la presenza della nuova voce.

Esempio: aggiornare un elenco con chiave usando un file CSV

È possibile fornire i valori per gli elenchi con chiave nei seguenti tre modi:

- Immettere manualmente i valori chiave
- Importare i valori chiave da un file CSV.
- Importare i valori chiave da uno specifico processo CA IT PAM

Utilizzare il seguente esempio come guida per aggiornare i valori in un qualsiasi elenco con chiave definito dall'utente, in cui i valori sono memorizzati in un foglio di calcolo di Excel salvato come elenco di valori separati da virgola (*.csv).

Per aggiornare un elenco con chiave usando un file CSV

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria, infine sulla cartella Elenco con chiave.
2. Espandere la cartella Elenco con chiave e selezionare l'elenco con chiave da aggiornare, ad esempio Default_Accounts, quindi fare clic su Esporta valori.

   Verrà visualizzata la finestra di dialogo Esporta con file.csv come nome file predefinito.
3. Selezionare la directory nella quale si desidera salvare il file esportato. Cambiare il nome del file, ad esempio Default_Accounts.csv, quindi fare clic su Salva.

   Viene visualizzato un messaggio di conferma.
4. Fare clic su OK.
5. Accedere al percorso del file CSV esportato, aprirlo e scorrere fino a visualizzare l'ultima colonna, quindi aggiungere la voce che si desidera includere. È possibile facoltativamente eliminare la colonna relativa a qualsiasi voce predefinita si desideri rimuovere dall'elenco con chiave per Default_Accounts.
6. Salvare e chiudere il file CSV e tornare all'interfaccia di CA User Activity Reporting Module.
7. Fare clic su Importa valori per l'elenco che si desidera aggiornare, ovvero in questo esempio l'elenco con chiave Default_Accounts.
8. Fare clic su Sfoglia, selezionare il file salvato e fare clic su Apri.
9. Fare clic su OK.

   Il file viene caricato. Scorrere fino in fondo l'elenco Valori per verificare la presenza della nuova voce.

Aggiornare un elenco con chiave con un processo di valori dinamici

Se si utilizzano i processi di CA IT PAM per generare un elenco di valori associati ad una chiave utilizzata nelle query di CA User Activity Reporting Module, eseguire in CA User Activity Reporting Module il processo di valori dinamici di IT PAM ed aggiornare i valori per una determinata chiave. L'importazione consente di risparmiare il tempo dell'inserimento manuale di tutti i valori per una data chiave. Quando si modificano i valori di una delle chiavi, è possibile aggiornare tali valori in CA User Activity Reporting Module selezionando la chiave e ripetendo l'importazione dei valori dinamici.

Configurare l'integrazione di CA IT PAM per i valori dinamici prima di importare da esso i valori dell'elenco con chiave.

Per importare i valori di un elenco con chiave da CA IT PAM

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria, infine sulla cartella Elenco con chiave.
2. Espandere la cartella Elenco con chiave e selezionare l'elenco con chiave che si desidera aggiornare.
3. Per creare una chiave per i valori da importare:
   a. Fare clic su Aggiungi nella parte superiore della tabella dei valori con chiave.

      La prima riga disponibile nella colonna Utente è selezionata.

   b. Fare clic sulla riga, quindi digitare il nome della nuova chiave.
   c. Fare clic su Salva.
4. Per aggiornare i valori dinamici per una chiave esistente:
   a. Selezionare la chiave.
   b. Fare clic su Importa elenco valori dinamici nella parte superiore del riquadro dei dettagli.

      Verrà visualizzata la finestra di dialogo Importa elenco valori dinamici.

   c. Inserire il nome del processo dei valori dinamici di IT PAM che genera i valori per la chiave selezionata e fare clic su OK.

      Verrà eseguito il processo associato di CA IT PAM, restituito un file con i risultati ed aggiornati i valori per la chiave selezionata.

   d. Fare clic su Salva.

Ulteriori informazioni:

Abilitare l'importazione di valori dinamici (a pagina 348)
Informazioni sui processi di valori dinamici (a pagina 348)
Creare un processo CA IT PAM per generare un elenco di valori (a pagina 349)
Configurare l'integrazione di CA IT PAM per i valori dinamici (a pagina 350)

Definire l'utilizzo degli elenchi con chiave per una query

È consigliabile tenere gli elenchi con chiave aggiornati con i valori correnti. Per aggiornare un elenco con chiave utilizzato in un particolare rapporto o avviso, identificare innanzitutto le query utilizzate nel rapporto o nell'avviso. Dopodiché, determinare l'elenco con chiave utilizzato nella query o query di origine. Le query che utilizzano un elenco con chiave fanno spesso riferimento al nome dell'elenco con chiave nel proprio nome. Ad esempio, esistono query il cui nome contiene le parole "Default Accounts" o "Privileged Group".

Per verificare l'utilizzo degli elenchi con chiave per una query

1. Aprire una copia della query per la quale si desidera verificare l'utilizzo degli elenchi con chiave nella procedura guidata Progettazione query.
2. Fare clic sul passaggio Filtri query e quindi sulla scheda Filtri avanzati.
3. Una query che utilizza un elenco con chiave sarà dotata di un filtro con l'operatore Keyed. Il valore è il nome dell'elenco con chiave, ad esempio Default_Accounts.
4. Fare clic su Annulla. La copia della query non verrà salvata.

Creare i valori chiave per i rapporti predefiniti

Alcune chiavi predefinite utilizzate nei rapporti predefiniti non dispongono di valori predefiniti. Per utilizzare in maniera efficace tali rapporti, occorre fornire valori per i rispettivi elenchi con chiave. È inoltre possibile aggiungere valori personalizzati agli elenchi con chiave *con* valori predefiniti.

Esempi di elenchi con chiave senza valori predefiniti:

- Critical_Assets
- DMZ_Hosts
- EPHI_Database
- Business_Critical_Sources

È possibile aggiungere valori a qualsiasi elenco con chiave manualmente o tramite importazione.

Ulteriori informazioni:

Aggiornare manualmente un elenco con chiave (a pagina 354)
Aggiornare l'elenco con chiave con esporta/importa: (a pagina 355)
Esempio: aggiornare un elenco con chiave usando un file CSV (a pagina 357)

Creazione di valori chiave per Critical_Assets

Questo argomento fornisce un esempio dell'aggiunta di valori personalizzati ad un elenco con chiave senza valori predefiniti. Lo stesso esempio può essere utilizzato per aggiungere valori ad altri elenchi con chiave esistenti.

Sono disponibili alcuni rapporti e query che consentono di monitorare le attività in base agli host critici di business. A tale scopo, occorre prima identificare gli host come valori nell'elenco dei valori chiave relativo a Critical_Assets.

I rapporti che utilizzano l'elenco Critical_Assets sono:

- Creazione account per Host critici di business
- Errore di accesso agli Host critici di business
- Sessioni di accesso risorsa per Host critici di business
- Accesso alla risorsa per Host critici di business
- Accesso al sistema per Host critici di business

I rapporti analoghi di CA Access Control, CA Identity Manager e CA SiteMinder utilizzano l'elenco con chiave Critical_Assets, ad esempio: CA Access Control - Creazione account da parte di Host critici di business.

Le query che utilizzano l'elenco Critical_Assets sono:

- (>5) Accessi per Account di amministrazione su sistemi critici durante le ore notturne dell'ultima giornata
- (>5) Accessi da parte di account di amministrazione su sistemi critici durante i fine settimana nel corso dell'ultima settimana
- Attività di eccezione di sistema

Se si crea una query personalizzata sulle risorse critiche, definire il filtro come segue:

Colonna	Operatore	Valore
dest_hostname	Con chiave	Critical_Assets

Per definire un filtro per altri elenchi con chiave, sostituire il valore con il valore di elenco desiderato. Ad esempio, è possibile impostare EPHI_Database come valore di filtro per filtrare i nomi host appartenenti a tale elenco con chiave.

Per creare valori chiave per Critical_Assets

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria, infine sulla cartella Elenco con chiave.
2. Espandere la cartella Elenco con chiave e selezionare Critical_Assets.
3. Selezionare una delle seguenti azioni per creare questo elenco:
   - Fare clic su Aggiungi valore ed immettere i nuovi valori da inserire nell'elenco con chiave.
   - Creare un foglio di lavoro di Excel con una riga, in cui ogni colonna è un valore singolo. Salvarlo come file .csv. Fare clic su Importa valori per importare l'elenco modificato.
   - Se i valori per questa chiave vengono generati dinamicamente dal processo CA IT PAM di valori dinamici, fare clic su Importa elenco valori dinamici.
4. Fare clic su Salva.

   I rapporti che utilizzano questo elenco con chiave generati dai processi pianificati inizieranno a rispecchiare i dati relativi ai valori aggiornati.

Personalizzare i valori con chiave per gli amministratori

Questo argomento fornisce un esempio dell'aggiunta di valori personalizzati ad un elenco con chiave predefinito con alcuni valori già impostati. Lo stesso esempio può essere utilizzato per aggiungere valori ad altri elenchi con chiave esistenti.

Per monitorare le attività, è possibile utilizzare i rapporti predefiniti e le query ad essi associate da parte degli amministratori. I valori predefiniti comprendono amministratore, root, sa e admin. Per personalizzare l'elenco, identificare altri account con privilegi di amministrazione presenti nell'ambiente come valori nell'elenco dei valori chiave per Amministratori.

Se si crea una query personalizzata che utilizza questa chiave, definire il filtro come segue:

Colonna	Operatore	Valore
dest_username	Con chiave	Amministratori

Per definire un filtro per altri elenchi con chiave, sostituire il valore con il valore di elenco desiderato. Ad esempio, è possibile impostare EPHI_Database come valore di filtro per filtrare i nomi host appartenenti a tale elenco con chiave.

Per personalizzare i valori con chiave di Amministratori

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria, infine sulla cartella Elenco con chiave.

   In fondo al riquadro principale verrà visualizzato un elenco delle chiavi a cui è possibile aggiungere valori definiti dall'utente.

2. Selezionare la chiave, Amministratori.

   Vengono visualizzati i valori predefiniti.

3. Per aggiornare questo elenco, effettuare una o più delle seguenti azioni:

   - Aggiornare manualmente l'elenco:
     - Fare clic su Aggiungi valore ed immettere un nuovo valore da inserire nell'elenco con chiave.
     - Selezionare un valore e fare clic su Rimuovi valore per eliminare il valore dall'elenco.
     - Selezionare un valore, fare clic su Modifica valore, modificare il valore e fare clic su OK.
   - Aggiornare l'elenco con esporta/importa:
     a. Fare clic su Esporta valori per esportare l'elenco corrente.
     b. Aprire l'elenco esportato, modificarne i valori e salvare il file.
     c. Fare clic su Importa valori per importare l'elenco modificato.
   - Fare clic su Importa valori per importare i valori in un file csv aggiornato.
   - Se i valori per questa chiave vengono generati dinamicamente dal processo CA IT PAM di valori dinamici configurato, fare clic su Importa elenco valori dinamici.

4. Fare clic su Salva.

   I rapporti che utilizzano questo elenco con chiave generati dai processi pianificati inizieranno a rispecchiare i dati relativi ai valori aggiornati.

Visualizzare un rapporto utilizzando un elenco con chiave

È possibile visualizzare i risultati di un rapporto prima di pianificarne la generazione. Alcuni rapporti predefiniti utilizzano elenchi con chiave in cui la chiave è predefinita, mentre i valori sono definiti dall'utente. Una volta importati o aggiunti i valori di una chiave, si consiglia di visualizzare il rapporto utilizzando l'elenco con chiave.

Per visualizzare un rapporto utilizzando un elenco con chiave

1. Fare clic sulla scheda Query e rapporti e sulla sottoscheda Rapporti.
2. Selezionare un rapporto che utilizza un elenco con chiave.
3. Visualizzare i risultati.

Capitolo 12: Avvisi

Questa sezione contiene i seguenti argomenti:

Informazioni relative agli avvisi (a pagina 366)
Utilizzo delle query con il tag Avviso (a pagina 367)
Identificare altre query da utilizzare per gli avvisi. (a pagina 369)
Personalizzare le query per gli avvisi (a pagina 370)
Considerazioni relative agli avvisi (a pagina 381)
Utilizzare i processi CA IT PAM di output di evento/avviso (a pagina 384)
Modalità di utilizzo delle trap SNMP (a pagina 423)
Creazione di un alert (a pagina 470)
Esempio: creazione di un avviso per Spazio su disco insufficiente (a pagina 479)
Esempio: creazione di un avviso per un evento di automonitoraggio (a pagina 484)
Esempio: inviare un messaggio di posta elettronica all'amministratore quando si arresta il flusso degli eventi (a pagina 487)
Configurazione della memorizzazione degli avvisi (a pagina 491)
Esempio: creazione di un avviso per Business_Critical_Sources (a pagina 491)
Modifica di un avviso (a pagina 494)
Abilitare o disabilitare gli avvisi (a pagina 494)
Eliminazione di un avviso (a pagina 495)

Informazioni relative agli avvisi

Gli avvisi sono rapporti specializzati che generano un evento quando le condizioni della query vengono soddisfatte. Possono essere utili per monitorare l'ambiente, poiché consentono notifiche automatiche per un'ampia gamma di situazioni e occorrenze. Ad esempio, è possibile impostare avvisi per recapitare informazioni sulle tendenze di eventi, tenere traccia dell'utilizzo dello spazio su disco o recapitare notifiche quando si superano le soglie di accesso fallito.

Gli avvisi sono un ottimo modo per passare in rassegna le grandi quantità di dati raccolti per quegli eventi su cui è necessario agire. È possibile utilizzare gli avvisi per notificare quasi tutto quello che accade nella propria rete di raccolta registri. È possibile creare avvisi che consentano di ricevere informazioni su picchi del traffico in arrivo o in uscita, sul traffico di porte specifiche, sull'accesso ad alcune risorse privilegiate, sulle modifiche alla configurazione di varie identità di rete come firewall, database o server fondamentali, e così via.

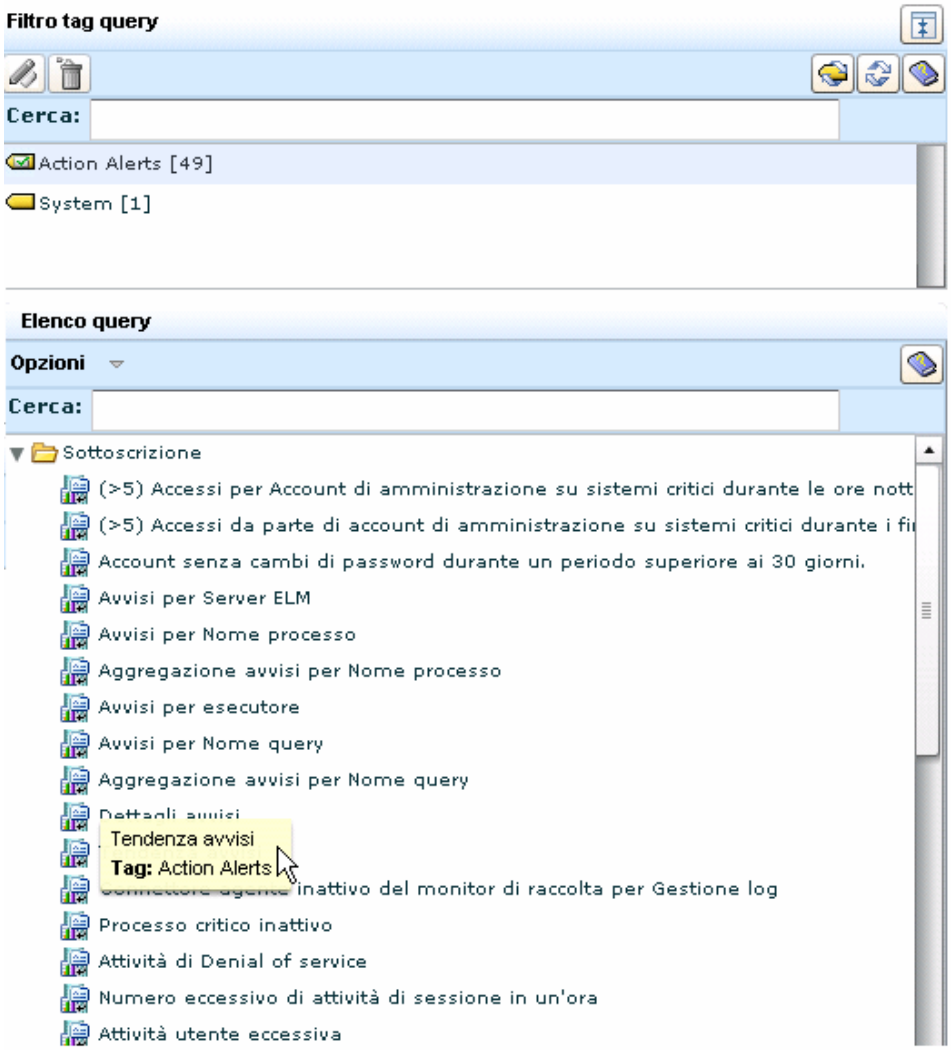
Gli avvisi possono essere creati nelle modalità seguenti:

- Utilizzo della procedura guidata di creazione avvisi
- Utilizzo della visualizzazione di una query
- Utilizzo di una query personalizzata

Le opzioni di pianificazione sono una parte significativa della creazione di un avviso, perché permettono di avere il controllo sulla durata e sulla frequenza dell'avvio dei processi di avviso.

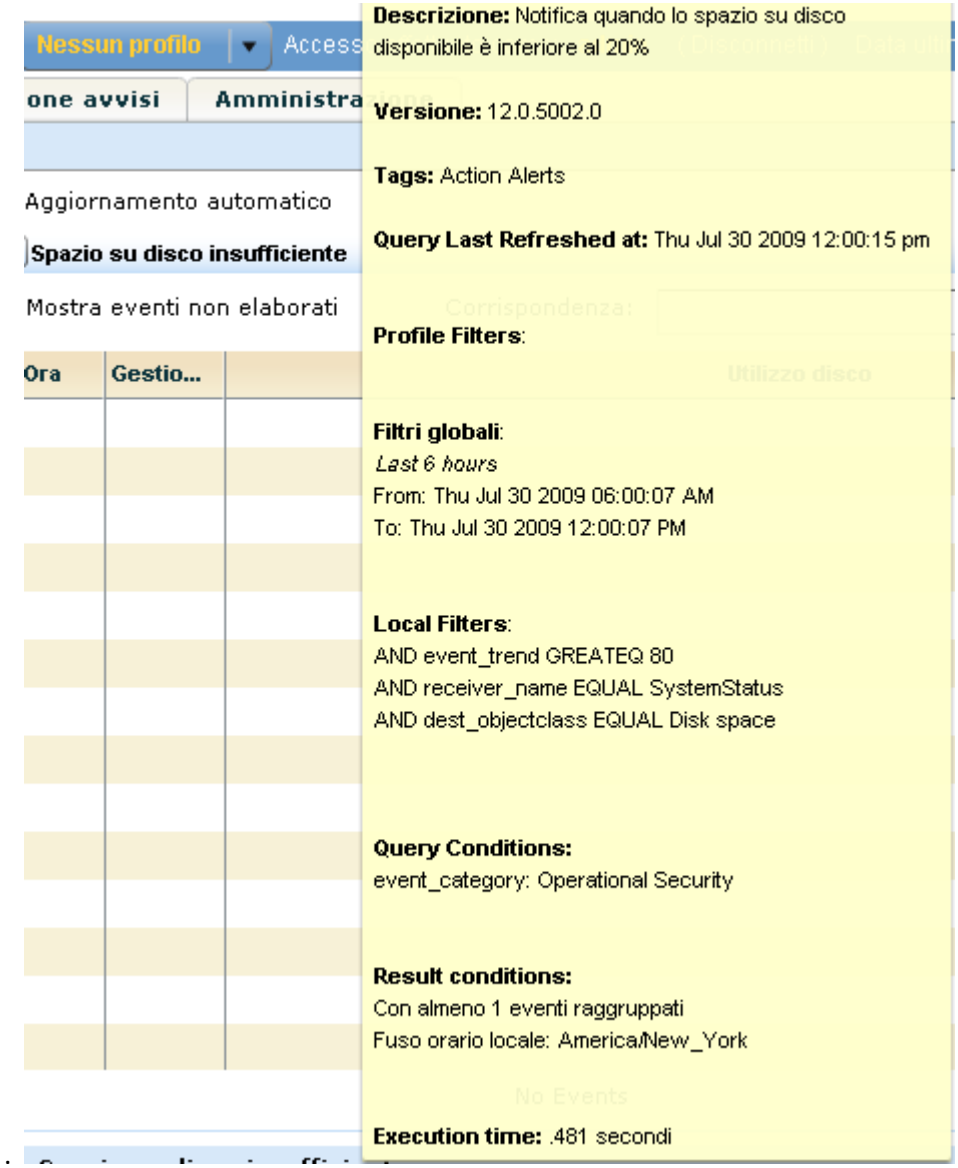
Utilizzo delle query con il tag Avviso

CA User Activity Reporting Module fornisce una serie di query con il tag Avvisi. Per visualizzare l'elenco delle query con tag Avvisi, fare clic sulla scheda Query e rapporti, quindi sulla sottoscheda Query e selezionare il tag Avvisi. Le query dotate di questo tag vengono visualizzate nell'Elenco query. Spostando il cursore sul nome di una query, verranno visualizzati i tag ad essa associati.



Prima di pianificare un avviso a partire da queste query, è possibile ottenere ulteriori informazioni sulla funzione di ogni query. Per visualizzare la descrizione e le informazioni su una query, ad esempio Spazio su disco insufficiente, selezionare la query dal relativo elenco e spostare il cursore sul nome della query.

Verrà visualizzato il riepilogo della query, che contiene una descrizione, i filtri associati e le condizioni della query.



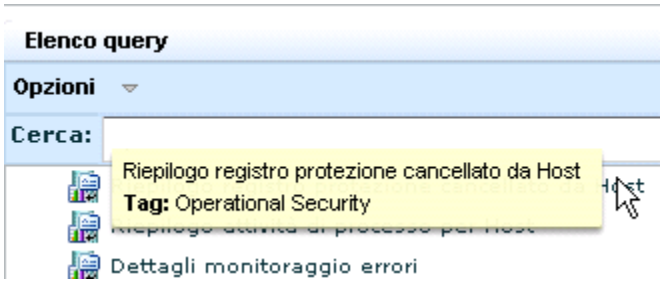
È possibile pianificare la query così com'è, oppure copiarla con un nuovo nome e personalizzarla in base alle proprie esigenze. Ad esempio, è possibile generare un avviso quando lo spazio disponibile su disco scende al di sotto del 25%, invece che del 20%. È possibile creare una query definita dall'utente basata sulla query predefinita e quindi selezionarla per il proprio avviso.

Nota: prima di utilizzare le query il cui titolo contiene le parole Gruppo con privilegi o Account predefinito, valutare se aggiungere valori chiave personali per gli elenchi con chiave corrispondenti.

Identificare altre query da utilizzare per gli avvisi.

Alcune query non contrassegnate come avvisi sono adatte ad essere inserite in un avviso pianificato, poiché consentono di recuperare solo gli eventi considerati gravi.

Ad esempio, Dettagli registro protezione cancellato da Host recupera tutti gli eventi in cui l'azione di evento è Registro protezione eliminato. L'unico tag per questa query è Sicurezza operativa.



L'azione Registro protezione eliminato è elencata nella CEG. La CEG definisce i seguenti due tipi di eventi con un livello di sicurezza mappato su 6, che corrisponde al livello grave.

Categoria	Classe	Azione	Risultato	Livello di protezione
Protezione operativa	Attività Registro protezione	Cancellazione registro protezione	Operazione riuscita	6
Protezione operativa	Attività Registro protezione	Cancellazione registro protezione	Operazione non riuscita	6

È consigliabile pianificare un avviso con questa query.

Ulteriori informazioni:

Identificare il filtro semplice per gli eventi di elevata gravità (a pagina 371)

Personalizzare le query per gli avvisi

Gli avvisi hanno la funzione di avvertire la persona, il processo o il prodotto appropriato in caso di evento grave. Nell'identificare le query su cui basare gli avvisi, prendere in considerazione le query progettate per recuperare gli eventi con livelli di sicurezza elevati.

Una volta identificate le definizioni degli eventi gravi, è possibile identificare le query in grado di recuperarli. Se le query non esistono, è possibile crearle.

Considerare la procedura seguente:

1. Identificare i tipi di eventi che CA considera molto gravi, in cui i tipi di evento sono definiti in base a categoria, classe, azione e risultato.
2. Identificare le query predefinite progettate per recuperare solo questo tipo di eventi.
3. Identificare le query predefinite progettate per recuperare gli eventi che potrebbero includere gli eventi gravi, ma possono essere personalizzate in modo da comprendere soltanto questi ultimi.
4. Creare query personalizzate dove non esistono query predefinite.
5. Pianificare gli avvisi in modo da eseguire frequentemente queste query.

Ulteriori informazioni:

Identificare il filtro semplice per gli eventi di elevata gravità (a pagina 371)
Personalizzare le query in modo da recuperare solo gli eventi gravi (a pagina 375)
Creare una query per recuperare solo gli eventi gravi (a pagina 373)

Identificare il filtro semplice per gli eventi di elevata gravità

Il livello di gravità degli eventi può variare da informativo a fatale. CA assegnerà un valore compreso fra 2 e 7 per indicare la gravità degli eventi in base al modello CEG di categoria, classe, azione e risultato. Il livello di gravità 7 è assegnato agli eventi di arresto del sistema. Il livello di gravità 6 è assegnato agli eventi con elevate implicazioni per la sicurezza o che richiedono attenzione immediata.

Se si prevede di creare query personalizzate o di personalizzare le query predefinite per utilizzarle negli avvisi, si consiglia di esaminare le definizioni del modello CEG relative ai tipi di evento gravi. La definizione del modello rappresenta la base per i filtri semplici. Questo significa che è possibile creare query che recuperano gli eventi in base alle informazioni di categoria, classe, azione e risultato di evento specificate dall'utente.

Per identificare il filtro semplice per gli eventi di gravità elevata

1. Fare clic sul collegamento della Guida in linea.
2. Espandere Grammatica comune evento e selezionare Assegnazione del livello di sicurezza.
3. Copiare la tabella in un foglio di calcolo ed ordinare il livello di sicurezza dal più alto al più basso.

   Nella tabella risultante saranno elencati i tipi di evento, iniziando dai più gravi stando al livello di sicurezza assegnato da CA.

   Segue un esempio: I risultati rispecchieranno le definizioni CEG correnti.

Categoria	Classe	Azione	Risultato	Livello di protezione
Protezione operativa	Attività di sistema	Chiusura del sistema	Operazione riuscita	7
Protezione operativa	Attività di sistema	Chiusura del sistema	Operazione non riuscita	7
Gestione configurazione	Gestione configurazione	Errore di configurazione	Operazione riuscita	6
Data Access	Gestione oggetti	Creazione file di controllo	Operazione riuscita	6
Host Security	Attività dell'antivirus	Errore di scansione	Operazione riuscita	6
Host Security	Attività dell'antivirus	Pulizia virus	Operazione non riuscita	6
Host Security	Attività dell'antivirus	Rilevato virus	Operazione riuscita	6
Host Security	Attività dell'antivirus	Quarantena virus	Operazione non riuscita	6
Host Security	Attività IDS/IPS	Violazione firma	Operazione riuscita	6
Network Security	Attività di violazione firma	Violazione firma	Operazione riuscita	6
Protezione operativa	Attività di sistema	Avvio sistema	Operazione non riuscita	6

Categoria	Classe	Azione	Risultato	Livello di protezione
Protezione operativa	Attività Registro protezione	Cancellazione registro protezione	Operazione riuscita	6
Protezione operativa	Attività Registro protezione	Cancellazione registro protezione	Operazione non riuscita	6
Accesso di sistema	Attività di autenticazione	Fallback autenticazione	Operazione non riuscita	6
Accesso di sistema	Attività di autenticazione	Avvio autenticazione	Operazione non riuscita	6

Creare una query per recuperare solo gli eventi gravi

È possibile creare una query da zero se non è presente una query predefinita in grado di recuperare i tipi di eventi di cui si desidera ricevere notifica. Considerare i seguenti tipi di eventi gravi:

Categoria	Classe	Azione	Risultato	Livello di protezione
Host Security	Attività dell'antivirus	Quarantena virus	Operazione non riuscita	6
Host Security	Attività IDS/IPS	Violazione firma	Operazione riuscita	6
Network Security	Attività di violazione firma	Violazione firma	Operazione riuscita	6

Esempio: creare una query per recuperare solo gli errori di quarantena dei virus

Si supponga, ad esempio, di voler ricevere una notifica per ogni errore di quarantena dei virus. Probabilmente, la parola chiave quarantena non compare nell'elenco di query. In questo caso, è possibile creare la query necessaria e pianificare un avviso che la esegue.

Per creare una query che recupera gli errori di quarantena dei virus

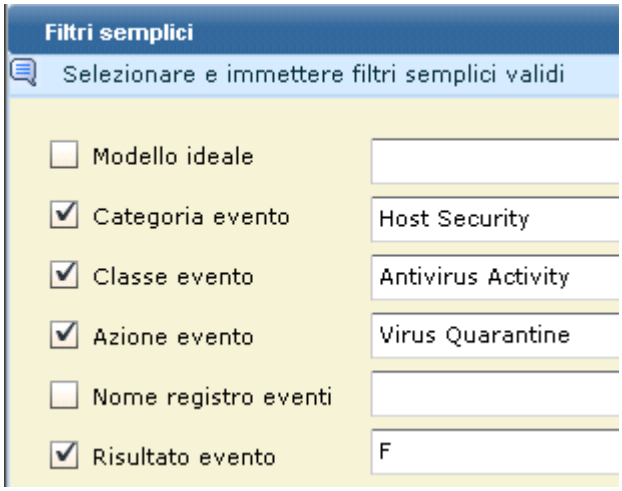
1. Fare clic su Query e rapporti.
2. In Opzioni elenco query selezionare Nuova.

   Verrà visualizzato il passaggio Dettagli della procedura guidata Progettazione query.
3. Inserire un nome.

   Ad esempio, inserire Avviso: errore quarantena virus
4. Aggiungere un tag personalizzato.

   Ad esempio, inserire Quarantena virus
5. Fare clic sul passaggio Colonne query ed aggiungere le colonne desiderate.
6. Selezionare il passaggio Filtri query.
7. Inserire un filtro semplice in base alla voce CEG dell'evento.

   Ad esempio, selezionare Sicurezza host come categoria, Attività antivirus come classe, Quarantena virus come azione e F come risultato.



8. Selezionare il passaggio Condizioni di risultato e selezionare Ultimi 5 minuti dal menu a discesa Intervalli predefiniti, in modo da garantire la tempestività dell'avviso.
9. Fare clic su Salva e chiudi.

Personalizzare le query in modo da recuperare solo gli eventi gravi

Le query predefinite non dotate di tag di avviso sono progettate per l'utilizzo con i rapporti. È normale che i rapporti contengano dati che rispecchiano eventi di tutti i livelli di gravità. È possibile personalizzare le query selezionate in modo da recuperare solo gli eventi gravi. Per fare ciò, identificare una query che recupera eventi gravi e meno gravi, copiarla, inserire filtri in grado di recuperare i soli eventi gravi e salvare la query per consentirne la selezione in un avviso.

Prima di iniziare, tenere a portata di mano il foglio di calcolo con l'elenco delle definizioni degli eventi gravi. L'esempio è basato sulle seguenti informazioni CEG:

Categoria	Classe	Azione	Risultato	Livello di protezione
Protezione operativa	Attività di sistema	Chiusura del sistema	Operazione riuscita	7
Protezione operativa	Attività di sistema	Chiusura del sistema	Operazione non riuscita	7

La query da personalizzare recupera gli eventi relativi all'arresto e all'avvio del sistema.

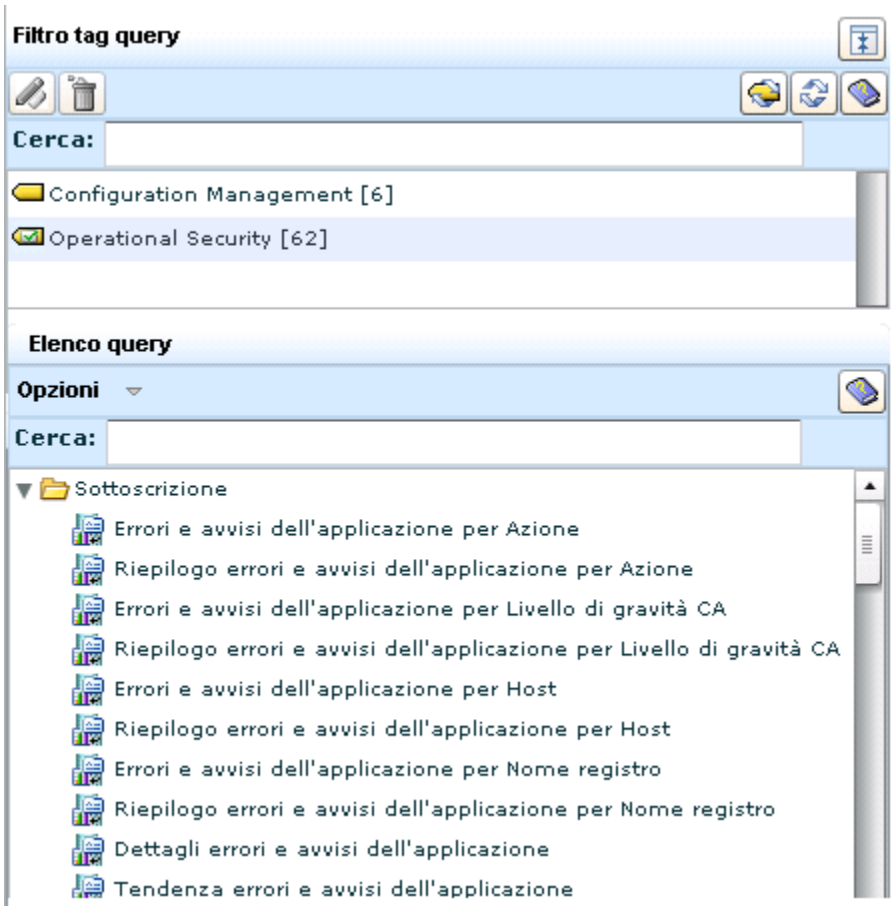
Per personalizzare una query in modo da recuperare solo gli eventi gravi

1. Fare clic sulla scheda Query e rapporti.
2. Selezionare un filtro di tag di query corrispondente alla categoria di un evento grave.

   Ad esempio, scegliere Sicurezza operativa.

3. Individuare nell'elenco le query con nomi contenenti parole chiave presenti nella classe o nell'azione del tipo di evento identificato.

   Ad esempio, le parole chiave Arresto del sistema compaiono nelle query che iniziano con la frase Avvio o arresto del sistema per host.



4. Copiare la query Dettagli di avvio o arresto del sistema per Host. Evidenziare la query e selezionare Copia dall'elenco a discesa Opzioni.
5. Fare clic su Filtri di query e confrontare le impostazioni predefinite con le voci di tabella per il tipo di evento grave.

   Per questa query, è selezionato solo Sicurezza operativa.
6. Fare riferimento alla tabella per i valori da inserire per classe ed azione.

   Ad esempio, selezionare Attività di sistema come classe e Arresto del sistema come azione.

7. Selezionare la scheda Filtri avanzati per stabilire se occorrono modifiche.

   Fare clic su Elimina per ogni riga, poiché il filtro event_action uguale ad avvio o arresto del sistema non è pertinente a questa query personalizzata.
8. Sostituire con un filtro per il risultato.

   Ad esempio, creare un filtro in cui event_result sia uguale a conferma o errore.

Logico	(	Colonna	Funzione	Operatore	Valore
		event_result		Uguale a	S
Or		event_result		Uguale a	F

9. Fare clic su Dettagli e denominare la query in modo da indicare l'intenzione di utilizzarla per un avviso.

   Ad esempio, inserire come nome Avviso: informazioni di arresto del sistema da parte dell'host. Modificare la descrizione di conseguenza.

10. Fare clic su Condizioni risultato. Per i casi più gravi, eseguire le query di frequente.

    Ad esempio, selezionare l'intervallo predefinito per gli ultimi 5 minuti, in modo da eseguire la query ogni 5 minuti nel caso si verifichi questo evento grave.

11. Fare clic su Salva.

    Con questa query è possibile creare un avviso per notificare una persona, un prodotto o un processo di conferma o mancato arresto del sistema. La notifica del prodotto viene eseguita attraverso trap SNMP, mentre quella del processo attraverso un output di evento/avviso di IT PAM.

Possibili query da modificare

Considerare la modifica delle query predefinite selezionate per utilizzarle con gli avvisi. Per personalizzare una query, aggiungere il filtro semplice in base all'analisi CEG. Impostare Selezione intervallo date con Intervallo predefinito Ultimi 5 minuti per garantire una notifica immediata. Seguono alcuni esempi:

Query per errore di configurazione

1. Copiare dettagli attività di errore configurazione.

   Questa query restituisce sia conferme che errori. Sono necessarie solo le conferme.

2. Impostare il filtro semplice come segue:

Categoria	Classe	Azione	Risultato	Livello di protezione
Gestione configurazione	Gestione configurazione	Errore di configurazione	Operazione riuscita	6

3. Salvare come Avviso: errore di configurazione

Query per conferma di creazione file di controllo

1. Copiare dettagli attività di modifica dei dati

   Questa query consente di recuperare tutte le azioni di accesso ai dati.

2. Impostare il filtro semplice come segue:

Categoria	Classe	Azione	Risultato	Livello di protezione
Data Access	Gestione oggetti	Creazione file di controllo	Operazione riuscita	6

3. Salvare come Avviso: Conferma di creazione file di controllo

Query per Errore di scansione antivirus

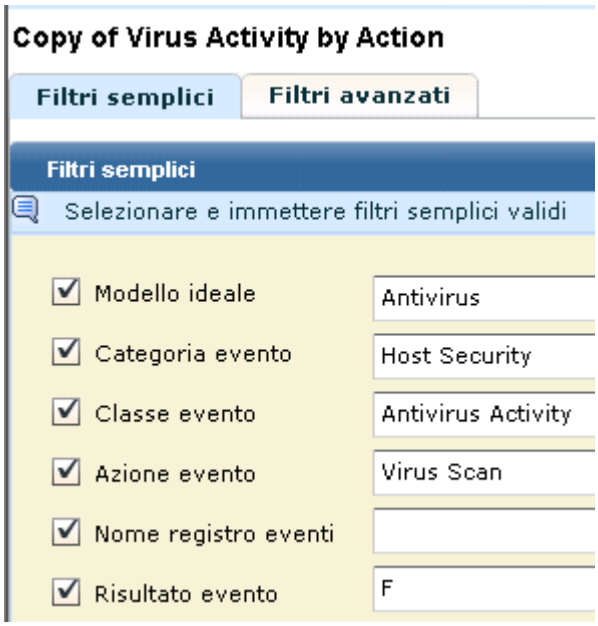
1. Copiare Attività virus per Azione

   Questa query consente di filtrare tutte le azioni di sicurezza dell'host antivirus.

2. Usare la seguente definizione come guida:

Categoria	Classe	Azione	Risultato	Livello di protezione
Host Security	Attività dell'antivirus	Errore di scansione	Operazione riuscita	6

3. Impostare il filtro semplice come segue:



4. Salvare come Avviso: errore di scansione virus

Query per Errore eliminazione virus

È possibile utilizzare la query predefinita Dettagli attività di rilevamento e disinfezione virus per Azione per recuperare le azioni con esito sia positivo che negativo. Ciò potrebbe essere sufficiente per le proprie esigenze. Facoltativamente, è possibile creare due query separate basate su questa, in cui specificare il risultato come indicato nella tabella CEG per gli eventi gravi.

1. Copiare Dettagli attività di rilevamento e disinfezione virus per Azione
2. Creare un filtro semplice per specificare il risultato dell'errore.

Categoria	Classe	Azione	Risultato	Livello di protezione
Host Security	Attività dell'antivirus	Pulizia virus	Operazione non riuscita	6

3. Eliminare il filtro avanzato.
4. Salvare come Avviso: Errore eliminazione virus

Query per Conferma individuazione di un virus

È possibile utilizzare la query predefinita Dettagli attività di rilevamento e disinfezione virus per Azione per recuperare le azioni con esito sia positivo che negativo. Ciò potrebbe essere sufficiente per le proprie esigenze. Facoltativamente, è possibile creare due query separate basate su questa, in cui specificare il risultato come indicato nella tabella CEG per gli eventi gravi.

1. Copiare Dettagli attività di rilevamento e disinfezione virus per Azione
2. Creare un filtro semplice per specificare il risultato di conferma solo con l'attività di individuazione.

Categoria	Classe	Azione	Risultato	Livello di protezione
Host Security	Attività dell'antivirus	Rilevato virus	Operazione riuscita	6

3. Eliminare il filtro avanzato.
4. Salvare come Avviso: virus individuato

Considerazioni relative agli avvisi

È possibile visualizzare i risultati di ogni avviso di CA User Activity Reporting Module senza alcuna configurazione particolare. Inoltre, è possibile inviare un avviso alle seguenti destinazioni:

- Feed RSS
- Destinatari di posta
- Destinazioni di trap SNMP, come CA Spectrum o CA NSM
- Un processo CA IT PAM di output di evento/avviso

Gli amministratori possono configurare tali destinazioni nella scheda Amministrazione, nella sottoscheda Servizi, in Configurazione globale o Configurazione globale di servizio: Server di rapporto.

Verificare che queste destinazioni siano configurate come segue prima di iniziare a pianificare un avviso.

- Per utilizzare il Lettore feed, verificare che non sia selezionata la casella di controllo Per visualizzare gli avvisi di azione è necessaria l'autenticazione in Configurazione globale.

  Segue l'URL del feed RSS, dove *elmhostname* è il nome host del server CA User Activity Reporting Module:

  ```
  https://{elmhostname}:5250/spin/calm/getActionQueryRssFeeds.csp
  ```

- Per inviare avvisi a destinatari di posta elettronica, verificare che la sezione Impostazioni di posta elettronica sia configurata in Configurazione globale di servizio: Server di rapporto.
- (Facoltativo) Per inviare avvisi alle destinazioni SNMP, verificare che la sezione Configurazione SNMP sia configurata in Configurazione di servizio globale: Server di rapporto.
- Per inviare avvisi al processo CA IT PAM di output di evento/avviso, verificare che la sezione CA IT PAM sia configurata in Configurazione globale di servizio: Server di rapporto. L'unico valore non necessario per gli avvisi è quello relativo processo Valori dinamici.

Quando si specificano le condizioni per i risultati di un avviso, prendere in considerazione quanto segue:

- Utilizzare le ore di inizio e di fine dinamiche preimpostate per gli intervalli predefiniti.
  - L'intervallo predefinito, ultimi 5 minuti, è impostato con l'ora di fine dinamica su "ora", "-2 minuti" e con l'ora di inizio dinamica su "ora", "-7 minuti". L'intervallo predefinito e gli altri intervalli di tempo preimpostati consentono il tempo necessario per il salvataggio degli eventi nel database.

    Nota: non modificare l'ora di fine dinamica in *"ora"* o in *"ora", "-1 minuti"*. La modifica del valore predefinito può causare la visualizzazione di dati incompleti al momento di aprire l'URL dalla destinazione. Ad esempio, se uno dei valori è il conteggio degli eventi, il conteggio visualizzato dall'URL potrebbe essere inferiore a quello visualizzato da CA User Activity Reporting Module.
- Se tramite l'impostazione predefinita vengono visualizzati dati incompleti, estendere l'ora di fine dinamica. Ad esempio, impostarla su "ora", "-10 minuti".

Quando si crea una pianificazione di avvisi, considerare quanto segue:

- L'intervallo di ricorrenza corrisponde alla frequenza di esecuzione della query. Pertanto, con un intervallo di ricorrenza di 5 minuti, la query verrà eseguita ogni cinque minuti, oppure 12 volte all'ora. Verrà generato un avviso solo se la query restituisce risultati al momento dell'esecuzione.
- Impostare l'intervallo di ricorrenza in base all'importanza della tempestività di risposta in caso di condizioni sperimentate.
  - Se occorre eseguire un'azione tempestiva per porre rimedio alla condizione, impostare l'intervallo di ricorrenza su una frequenza elevata in modo da ricevere una notifica il più presto possibile.
  - Se si desidera tenere traccia della condizione, ma senza intervenire in alcun modo, impostare l'intervallo di ricorrenza su una frequenza bassa.
- Non impostare l'intervallo di ricorrenza su una frequenza elevata, ad esempio ogni cinque minuti, se l'ora del server CA User Activity Reporting Module non è sincronizzata con il server NTP.

  Importante: Per ottenere risultati completi quando si imposta l'esecuzione della query con frequenza elevata, occorre sincronizzare l'ora del server CA User Activity Reporting Module con il server NTP.

Prendere in considerazione le seguenti opzioni di filtraggio:

- Per utilizzare i filtri definiti con le query incluse, non serve alcuna azione.
- Per applicare filtri aggiuntivi alle query incluse in un avviso, definirli al passaggio Filtri di avviso.
- Per applicare lo stesso gruppo di filtri a più processi di avviso, utilizzare un profilo.

Prima di configurare le soglie per gli avvisi su un server di rapporto CA User Activity Reporting Module, considerare quanto segue:

- Per mantenere il feed RSS a dimensioni ragionevoli, impostare il numero massimo di avvisi consentiti. Più frequenti saranno gli intervalli di ricorrenza degli avvisi abilitati e più rapidamente il feed si riempirà, qualora la query o le query restituiscano risultati.
- Per verificare che il feed RSS non conservi gli avvisi per un tempo eccessivo, impostare la conservazione degli avvisi sul numero massimo dei giorni per i quali conservare un record.
- Tenere presente la frequenza con cui si desidera controllare la presenza di avvisi nel feed. Questa frequenza può essere utile per pianificare la durata della memorizzazione dei record.
- Per fare in modo che nel feed RSS sia sempre visualizzato il risultato più recente di tutti i processi, configurare i valori di conservazione in modo che gli avvisi eseguiti poco frequentemente non siano cancellati perché più vecchi di quelli eseguiti più di frequente, che riempiono la coda fino alla capacità massima.

Ulteriori informazioni:

Configurazione della memorizzazione degli avvisi (a pagina 491)
Esempio: creazione di un avviso per Spazio su disco insufficiente (a pagina 479)

Utilizzare i processi CA IT PAM di output di evento/avviso

Per utilizzare i processi CA IT PAM di output di evento/avviso integrati con CA User Activity Reporting Module, è necessario utilizzare una combinazione delle seguenti attività:

- Importare il processo di output di evento/avviso campione.
- Creare processi di output di evento/avviso in CA IT PAM che soddisfano i requisiti di integrazione
- Configurare l'integrazione di CA IT PAM e specificare il processo di output di evento/avviso predefinito
- Eseguire i processi di ouput di evento/avviso a partire dai risultati selezionati della query
- Pianificare gli avvisi che eseguono un processo CA IT PAM per riga
- Pianificare gli avvisi che eseguono un processo CA IT PAM per query

Ulteriori informazioni:

Importazione del processo di output di evento/avviso campione (a pagina 393)
Linee guida per la creazione di un processo di output di evento/avviso (a pagina 401)
Esempio: eseguire un processo di output di evento/avviso con i risultati della query selezionata (a pagina 409)
Esempio: inviare un avviso che esegue un processo IT PAM per riga (a pagina 415)
Esempio: inviare un avviso che esegua un processo di IT PAM per query (a pagina 420)

Informazioni sui processi CA IT PAM di output di evento/avviso

CA User Activity Reporting Module individua gli eventi che richiedono un intervento. È possibile generare avvisi non appena si verificano eventi indesiderati. L'integrazione con CA IT PAM consente ad un avviso di eseguire un processo di output di evento/avviso. I processi di output di evento/avviso sono progettati per richiamare le appropriate azioni correttive da parte di altri prodotti. In altre parole, i processi di output di evento/avviso sono processi CA IT PAM che comandano ad altri prodotti di eseguire azioni specifiche su specifici oggetti.

CA User Activity Reporting Module, CA IT PAM e le applicazioni di terze parti operano sinergicamente per proteggere l'ambiente dell'utente. CA User Activity Reporting Module automatizza l'individuazione di eventi indesiderati ed il processo CA IT PAM di output di evento/avviso richiama altri prodotti per mettere in atto una serie adeguata di risposte.

L'integrazione comprende la configurazione della connessione al server di CA IT PAM per specificare l'esecuzione del processo ed i parametri di processo con i valori predefiniti.

È possibile eseguire il processo CA IT PAM su richiesta a partire da un risultato di query visualizzato (riga) oppure mediante avvisi pianificati. In entrambi i casi, valori di parametro come riepilogo e descrizione possono essere adattati in modo da fornire informazioni di supporto al prodotto di destinazione del processo CA IT PAM.

Ulteriori informazioni:

Architettura che supporta l'integrazione di CA IT PAM (a pagina 386)
Lavorare con i processi di output di evento/avviso (a pagina 386)
Come opera l'integrazione di CA IT PAM (a pagina 388)
Esempio: flusso dati per l'elaborazione di output di evento/avviso (a pagina 391)

Architettura che supporta l'integrazione di CA IT PAM

Per eseguire un processo di output di evento/avviso di CA IT PAM a partire da un avviso, è necessario disporre dei seguenti componenti di rete:

- Un ambiente CA User Activity Reporting Module funzionale, ad esempio:
  - Agenti con connettori in grado di acquisire eventi non elaborati dalle origini evento
  - Server CA User Activity Reporting Module di raccolta in grado di perfezionare gli eventi non elaborati e di inviarli ai server di rapporto
  - Server CA User Activity Reporting Module di rapporto in grado di elaborare gli avvisi pianificati e le query su richiesta
- Un server CA IT Process Automation Manager r2.1 (CA IT PAM) configurato con processi che richiamino un altro prodotto per eseguire un'azione correttiva di routine
- Un server con un prodotto utilizzato dal processo CA IT PAM, ad esempio un server con un prodotto help desk

Lavorare con i processi di output di evento/avviso

Segue una panoramica del flusso di lavoro associato all'utilizzo di un processo di output di evento/avviso di CA IT PAM:

1. Determinare se impostare l'integrazione di CA IT PAM con o senza processo campione. Il vantaggio di utilizzare il processo campione consiste nella possibilità di visualizzare immediatamente i risultati. È possibile rimandare l'aggiornamento del processo in uso finché non si avrà acquisito familiarità con i risultati dell'integrazione. Per utilizzare il processo campione, è necessario disporre di CA Service Desk.
2. Eseguire una o entrambe le seguenti operazioni:
   - Importare il processo campione e specificare i parametri di connessione di CA ServiceDesk
   - Creare processi di output di evento/avviso che soddisfino i requisiti di integrazione di CA User Activity Reporting Module

3. Raccogliere le informazioni per l'integrazione di CA IT PAM dal processo campione o da quello creato dall'utente.
4. Configurare l'integrazione di CA IT PAM per l'output di evento/avviso.
5. Verificare che gli utenti che controllano i risultati del processo di output di evento/avviso nel prodotto di terze parti dispongano di account utente di CA User Activity Reporting Module e siano a conoscenza delle credenziali di accesso. È possibile assegnare il ruolo di Revisore a questo tipo di account.

   Nota: al momento dell'accesso, gli utenti potranno solo visualizzare la pagina con i risultati della query associati.
6. Preparare l'automazione dell'esecuzione di un processo di output di evento/avviso.
   a. Identificare una o più query che restituiscono i dati su cui il prodotto di terze parti può eseguire operazioni, in base al processo di CA IT PAM configurato.
   b. Se la query utilizza un elenco con chiave, verificare che quest'ultimo contenga i valori necessari.
   c. Eseguire il processo di output di evento/avviso sui risultati della query e verificarne l'esito.
7. Pianificare un avviso di azione utilizzando la procedura documentata e le seguenti linee guida.
   a. Al passaggio per la selezione dell'avviso:
      - Inserire un nome processo.
      - Verificare che il tipo di selezione sia Query.
      - Selezionare le query identificate durante la pianificazione.
   b. Al passaggio Destinazione, selezionare la scheda Processo CA IT PAM e specificare le informazioni di output evento/avviso come segue:
      - Selezionare le query su cui basare l'avviso.
      - Specificare se eseguire il processo una volta per ogni query che restituisca risultati oppure una volta per ogni riga restituita.
      - Specificare i valori dei parametri del processo IT PAM. È possibile inserire i valori ed il testo dei parametri di riepilogo e descrizione solo se si esegue il processo per ogni riga.
   c. Specificare le informazioni per i passaggi restanti, come per ogni avviso di azione pianificato, e quindi salvare e chiudere la procedura guidata.

8. Controllare i risultati:
   a. Verificare che il processo in questione sia incluso nell'elenco Processi di avviso.
   b. Controllare gli eventi di automonitoraggio e l'azione Notifica evento per verificare che l'esito dell'esecuzione del processo IT PAM sia positivo.
   c. (Facoltativo) Accedere al prodotto di terze parti che ha risposto alle informazioni di output di evento/avviso di CA User Activity Reporting Module trasmesse dal processo IT PAM.

Ulteriori informazioni:

Importazione del processo di output di evento/avviso campione (a pagina 393)
Linee guida per la creazione di un processo di output di evento/avviso (a pagina 401)
Esempio: eseguire un processo di output di evento/avviso con i risultati della query selezionata (a pagina 409)
Progettare le query di eventi da inviare al processo di output di evento/avviso (a pagina 413)
Impostare le destinazioni di notifica (a pagina 474)
Esempio: inviare un avviso che esegue un processo IT PAM per riga (a pagina 415)

Come opera l'integrazione di CA IT PAM

Supporre che si verifichi la seguente configurazione:

- CA IT PAM è stato configurato sulla pagina di configurazione del server di rapporto ed è stata specificata l'esecuzione del processo di output di evento/avviso.
- È stato pianificato un avviso con CA IT PAM come destinazione ed è stata impostata l'esecuzione del processo una volta per ogni riga. Per i parametri che consentono di immettere istruzioni di riepilogo e descrizione, le istruzioni immesse dall'utente comprendono campi CEG.
- È stato pianificato un altro avviso con CA IT PAM come destinazione, indicando l'esecuzione del processo una volta per ogni query. Per i parametri che consentono di immettere istruzioni di riepilogo e descrizione, è stato inserito testo letterale.

Il processo end-to-end comprende le azioni di più origini:

- La generazione di eventi non elaborati da parte delle origini evento
- La raccolta ed il perfezionamento degli eventi da parte di CA User Activity Reporting Module
- La generazione di avvisi quando gli eventi potenziati soddisfano i criteri di query di CA User Activity Reporting Module
- L'invio di output di evento e di avviso a CA IT PAM tramite CA User Activity Reporting Module
- L'esecuzione del processo di output di evento/avviso configurato da parte di CA IT PAM su un sistema di terze parti
- Uno dei seguenti elementi:
  - La valutazione dei dati da parte di un utente del sistema di terze parti che definisce ed esegue l'azione corretta da intraprendere.
  - La risposta automatica da parte di tale sistema di terze parti al verificarsi degli eventi.

Di seguito è riportata una sintesi dell'elaborazione:

1. Le origini evento producono eventi non elaborati.
2. Gli agenti raccolgono alcuni di questi eventi non elaborati in base ai connettori e li trasferiscono verso un server di raccolta.
3. Il server di raccolta normalizza e classifica gli eventi non elaborati, trasferendo gli eventi potenziati ad un server di rapporto.

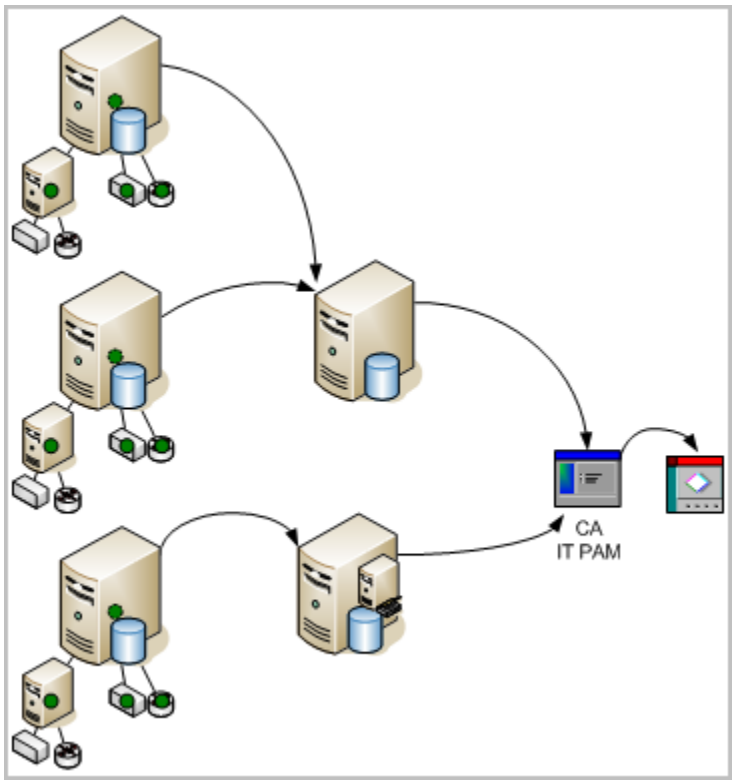
   Ad esempio, quando si modifica la configurazione di qualsiasi sistema, verrà creato un registro successivamente classificato come modifica di configurazione. L'evento acquisisce l'ora della modifica, l'host in cui è stata eseguita, l'utente che l'ha effettuata ed il risultato del tentativo di modifica.
4. Il server di rapporto eseguirà le query selezionate per ogni avviso pianificato.

5. Se gli eventi perfezionati soddisfano i criteri di query, verrà generato un avviso e le seguenti informazioni verranno trasferite dal server di rapporto a CA IT PAM:
   - Dettagli avviso
     - I parametri di processo visualizzati e relativi valori
     - I campi CEG inviati per i parametri di processo non visualizzati
   - Dettagli evento
     - Per ogni riga, i dettagli evento vengono trasmessi dalle voci nei campi disponibili delle istruzioni di riepilogo e descrizione, in cui gli utenti descrivono gli eventi utilizzando le variabili dei campi CEG che compongono la query selezionata per l'avviso.
     - Per ogni query, i dettagli evento vengono trasmessi con un URL in una pagina di CA User Activity Reporting Module in cui verranno visualizzati a livello di riga.
6. Se l'invio viene completato con successo, CA IT PAM prosegue con l'elaborazione in base a quanto definito nel processo di output di evento/avviso configurato.
7. Se il prodotto di terze parti è CA Service Desk ed il processo di output di evento/avviso è quello campione, si verificheranno le seguenti condizioni:
   - Verrà aperto un ticket dell'help desk con un numero assegnato. I campi sul ticket verranno compilati con i valori di parametro della definizione di avviso. Se si riceve un URL, esso verrà visualizzato con l'istruzione di riepilogo.
   - CA Service Desk restituirà il numero di ticket a CA IT PAM
8. A sua volta, CA IT PAM trasmetterà il numero di ticket a CA User Activity Reporting Module
9. CA User Activity Reporting Module visualizzerà il numero di ticket come evento di automonitoraggio.

Esempio: flusso dati per l'elaborazione di output di evento/avviso

Le frecce indicate sul seguente diagramma illustrano il flusso dei dati:

- Dai server di raccolta ai server di rapporto
- Dai server di rapporto a CA IT PAM
- Da CA IT PAM al prodotto al quale il processo CA IT PAM invia l'output di CA User Activity Reporting Module, ad esempio CA Service Desk.

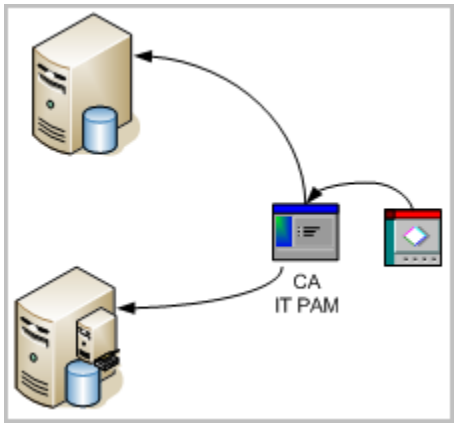


Quando CA User Activity Reporting Module riceve l'avviso di conferma dell'invio, verrà eseguito il polling di CA IT PAM per individuare lo stato del processo eseguito. Non appena inviato l'aggiornamento di stato da CA IT PAM, in CA User Activity Reporting Module verrà creato un evento di automonitoraggio con il risultato. La sequenza di elaborazione è la seguente:

1. CA IT PAM comunica a CA User Activity Reporting Module l'esito positivo o negativo del processo.
2. CA User Activity Reporting Module genera un evento di automonitoraggio di creazione notifica con il risultato ricevuto.

Tenere in considerazione l'esempio in cui il processo CA IT PAM crea un ticket dell'help desk con i valori di parametro del processo ed i dati di evento recuperati dalla query. Le frecce del seguente diagramma illustrano il seguente flusso dati:

- Dal prodotto help desk a CA IT PAM
- Da CA IT PAM ai server CA User Activity Reporting Module di rapporto di origine



Importazione del processo di output di evento/avviso campione

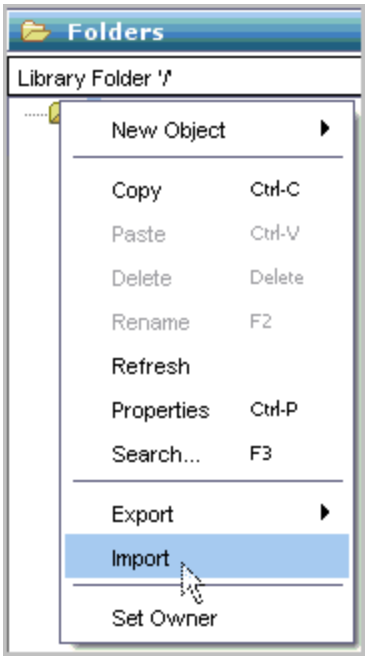
Per eseguire un test dell'integrazione di CA IT PAM e per acquisire familiarità con la procedura di configurazione tramite valori noti, è disponibile un processo campione. Tale processo si trova nel DVD, insieme all'applicazione. L'utilizzo di questo processo campione di CA IT PAM presuppone l'utilizzo di CA Service Desk come applicazione help desk.

È possibile configurare CA IT PAM in CA User Activity Reporting Module ed eseguire un test dell'esecuzione di questo processo campione di CA IT PAM con risultati di query selezionati dall'utente. Una volta acquisita familiarità con il funzionamento di CA User Activity Reporting Module con CA IT PAM, è possibile garantire la conformità del proprio processo e sostituire i valori di configurazione di CA IT PAM in modo da integrare la propria produzione.

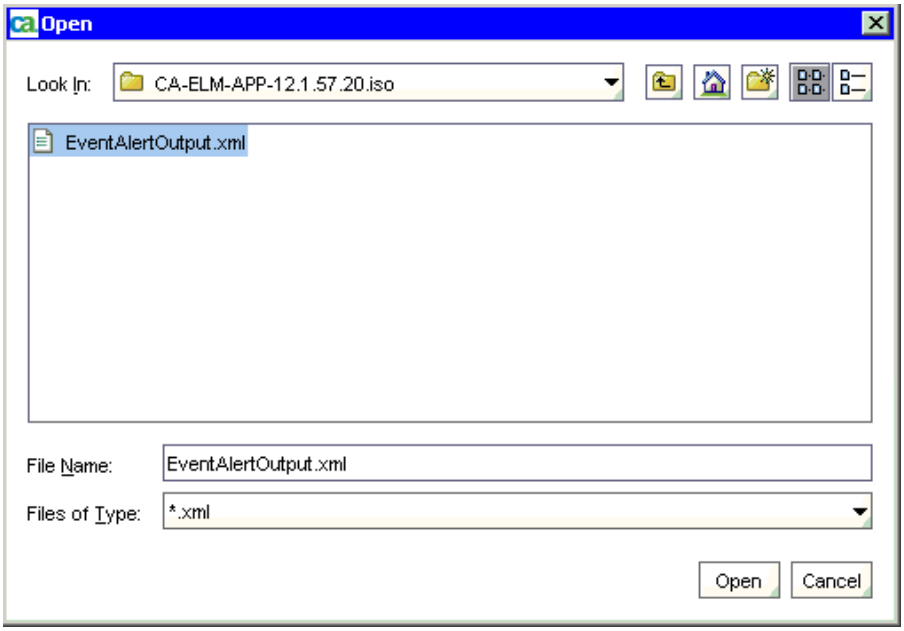
Per importare un processo campione ed eseguire un test dell'integrazione di IT PAM

1. Avviare CA IT PAM ed eseguire l'accesso.
2. Avviare il client ITPAM.

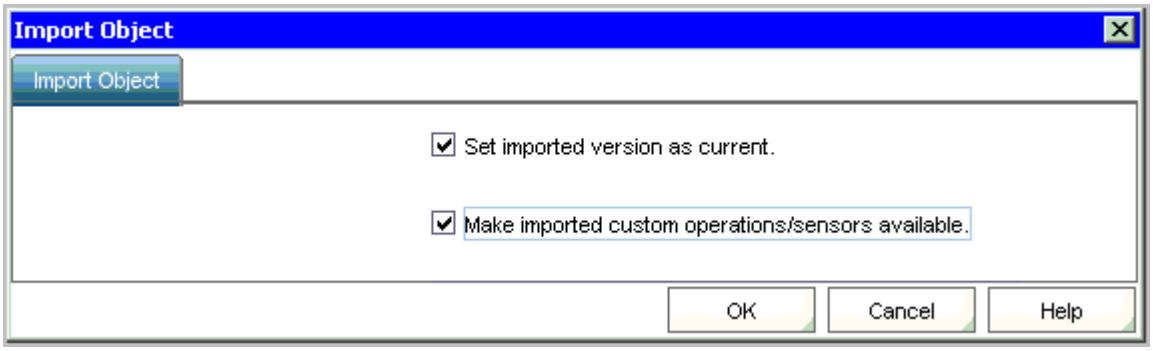
3. Importare il processo CA IT PAM campione, ovvero EventAlertOutput.xml, che si trova sul DVD dell'applicazione in CA/ITPAM. Questo campione dispone di tutti i valori necessari.
   a. Selezionare File, Apri browser di libreria.
   b. Fare clic su Cartelle nel riquadro di sinistra e fare clic su Importa nella cartella principale.



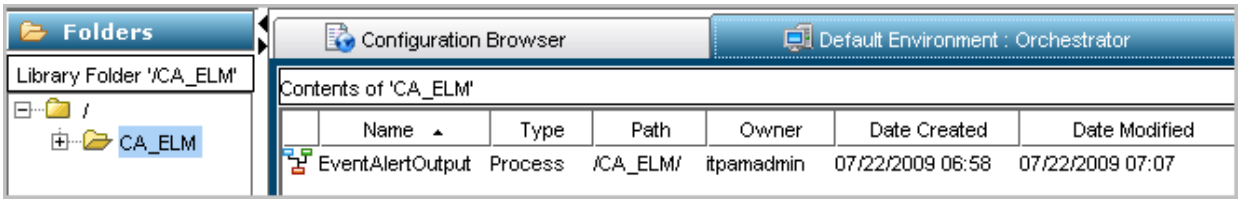
c. Selezionare il processo CA IT PAM campione, ossia EventAlertOutput.xml, dall'immagine ISO estratta e fare clic su Apri.



d. Selezionare entrambe le opzioni della finestra di dialogo Importa oggetto e fare clic su OK.



Verranno visualizzati il nome ed il percorso. Ad esempio, il nome è EventAlertOutput ed il percorso /CA_ELM/.



4. Specificare i parametri di connessione di Service Desk.
   a. Per visualizzare i parametri di connessione di Service Desk, fare clic sulla scheda Parametri di connessione di Service Desk di Request_Create.
   b. Utilizzare la seguente sintassi per specificare l'URL di Service Desk:

      ```
      http://<server name>:8080/axis/services/USD_R11_WebService
      ```

   c. Inserire come ID utente e password credenziali valide per l'accesso a Service Desk.
5. (Facoltativo) Eseguire un test del processo importato per verificare che funzioni in maniera indipendente.
6. Per uscire da CA IT PAM, chiudere il client ITPAM e fare clic Chiudi sessione.

Visualizzare il processo di output di evento/avviso campione

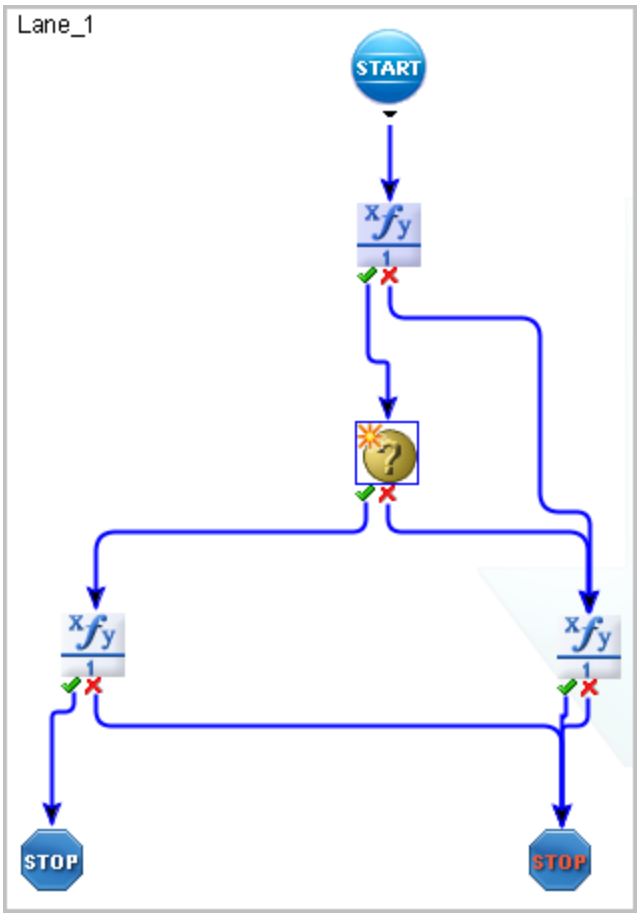
Se si importa il processo di output di evento/avviso campione, è possibile esaminarne la struttura in CA IT PAM. Attenersi alle seguenti linee guida per acquisire familiarità con i requisiti di CA User Activity Reporting Module nel contesto del processo campione. Nel corso della spiegazione, si vedrà dove definire i parametri di connessione del servizio Web e come definire gli operatori di calcolo. Inoltre, saranno presenti requisiti specifici di prodotto. Ad esempio, per configurare CA Service Desk come prodotto di terze parti occorre utilizzare l'operatore Request_Create da CA Service Desk Module ed un operatore di precalcolo che conserva i valori di gravità e priorità.

Per acquisire familiarità con il processo di output di evento/avviso campione

1. Visualizzare il modello del processo di destinazione.
   a. Avviare CA IT PAM ed eseguire l'accesso.
   b. Fare clic su Client ITPAM.
   c. Dal menu File, selezionare Apri browser di libreria.
   d. Nella scheda Cartelle, selezionare la cartella di libreria contenente il modello del processo di destinazione.

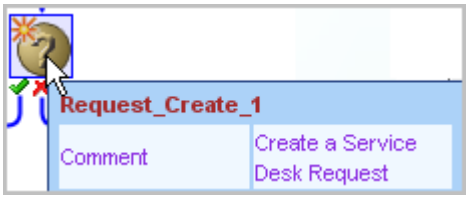
      Il nome ed il percorso del processo verranno visualizzati nel riquadro principale.
   e. Fare doppio clic sulla riga contenente il nome ed il percorso del processo.

Verrà visualizzato un modello simile al seguente: Questo modello di esempio contiene i requisiti minimi per CA User Activity Reporting Module.



2. Verificare che i parametri base di ServiceDesk soddisfino i requisiti di CA User Activity Reporting Module.

   a. Fare doppio clic sull'icona Request_Create_1.

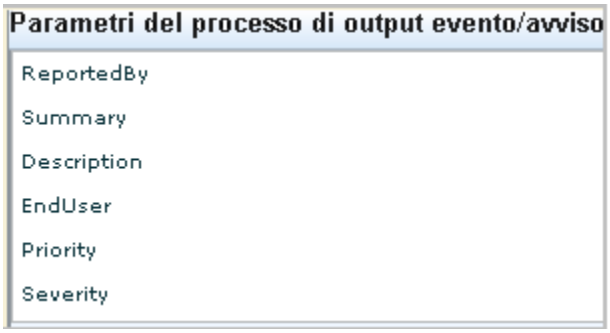


   L'operatore Request_Create trasmetterà i dati restituiti dalla query di avviso al prodotto di destinazione (applicazione). È necessario un operatore simile per ogni processo da eseguire in CA User Activity Reporting Module.

b. Nei parametri di base di ServiceDesk, i parametri di processo locali devono essere specificati con la seguente sintassi:

```
BasicParameter = Process.LocalParameter
```

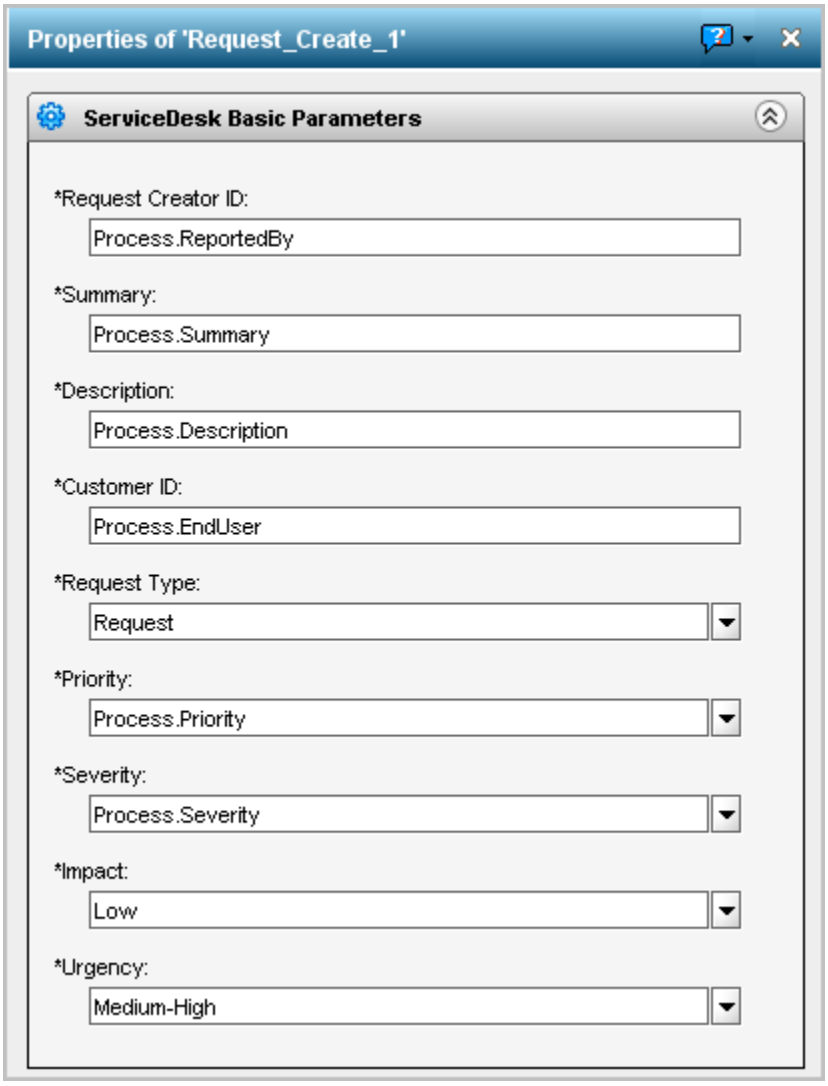
Nota: i parametri di processo locali corrispondono ai parametri del processo di output di evento/avviso aggiunti a CA User Activity Reporting Module dall'utente al momento della configurazione di CA IT PAM.



c. Poiché l'applicazione di destinazione è CA Service Desk, i seguenti parametri di processo locali vengono definiti come descritto nella seguente tabella:

Parametro di base di ServiceDesk	Parametro locale	Campo Service Desk	Note
ID dell'autore della richiesta	Process.ReportedBy	Assignee,Reported By	Un contatto valido di CA Service Desk
Riepilogo	Process.Summary	Riepilogo	Lasciare vuoto
Descrizione	Process.Description	Descrizione	Lasciare vuoto
ID cliente	Process.EndUser	Utente finale interessato	Un contatto valido di CA Service Desk
Priorità	Process.Priority	Priorità	1-5
Severity	Process.Severity	Severity	1-5

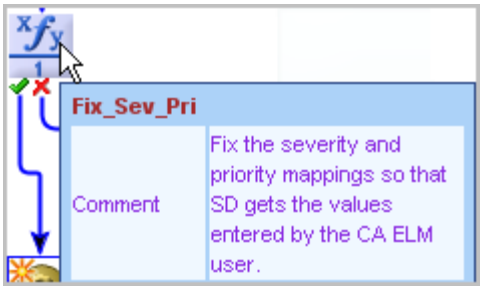
Il seguente esempio mostra i parametri locali validi per i parametri di base di ServiceDesk. Le voci fanno distinzione fra caratteri maiuscoli e minuscoli. Ovvero, Process.ReportedBy deve essere immesso esattamente come illustrato, con una R e una B maiuscole.



3. Per visualizzare i parametri di connessione di ServiceDesk, fare clic sulla scheda Parametri di connessione di Service Desk per Request_Create.
   - URL Service Desk:"http://<server name>:8080/axis/services/USD_R11_WebService"
   - ID utente Service Desk:"<SD user>"
   - Password:"<SD password>"

4. Per CA Service Desk è necessario un adattamento per garantire che i valori di gravità e priorità immessi in CA User Activity Reporting Module siano interpretati correttamente da CA Service Desk.

   a. Verrà visualizzato un operatore di precalcolo dopo Avvio e prima dell'operatore Create_Process. Nell'esempio seguente, tale operatore è denominato Fix_Sev_Pri.



   b. In Proprietà, Calcola, verranno definite le seguenti mappature:

```
if (Process.Priority == 1) Process.Priority = "pri:504";
else if (Process.Priority == 2) Process.Priority = "pri:503";
else if (Process.Priority == 3) Process.Priority = "pri:502";
else if (Process.Priority == 4) Process.Priority = "pri:501";
else if (Process.Priority == 5) Process.Priority = "pri:500";
```

```
if (Process.Severity == 1) Process.Severity = "sev:800";
else if (Process.Severity == 2) Process.Severity = "sev:801";
else if (Process.Severity == 3) Process.Severity = "sev:802";
else if (Process.Severity == 4) Process.Severity = "sev:803";
else if (Process.Severity == 5) Process.Severity = "sev:804";
```

5. I seguenti parametri di valore restituito o interfaccia di output sono formattati secondo quanto necessario in CA User Activity Reporting Module:

   - ResultString
   - FaultString

6. Visualizzare l'operatore di calcolo di conferma della creazione della richiesta. Questo formato deve essere utilizzato per ogni processo di output di evento/avviso da eseguire in CA User Activity Reporting Module.
   a. Fare clic sull'icona dell'operatore di calcolo per confermare la creazione della richiesta.
   b. Selezionare la scheda Calcola e fare clic su ... nel campo del codice sorgente.
   c. Si noti il modo in cui l'operatore di calcolo di conferma è definito nel codice sorgente:

      ```
      Process.ResultString = "Richiesta " + Request_Create_1.newRequestNumber +
      " creato in CA Service Desk.";
      ```

7. Visualizzare l'operatore di calcolo per l'errore. Questo formato è necessario per ogni processo di output di evento/avviso da eseguire in CA User Activity Reporting Module.
   a. Fare clic sull'icona dell'operatore di calcolo per l'errore.
   b. Selezionare la scheda Calcola e fare clic su ... nel campo del codice sorgente.
   c. Si noti il modo in cui l'operatore di calcolo dell'errore è definito nel codice sorgente, in cui Process.FaultString è mappato alla variabile SOAP corretta:

      ```
      Process.FaultString = Request_Create_1.SoapErrorResponse;
      ```

Linee guida per la creazione di un processo di output di evento/avviso

Per eseguire un processo di CA IT PAM da CA User Activity Reporting Module occorre seguire determinate linee guida. Prima di eseguire un processo di CA IT PAM da CA User Activity Reporting Module, verificare che includa i seguenti elementi:

- I parametri di connessione del servizio Web.
- Un operatore di calcolo Success per la mappatura della stringa Process:ResultString a un'istruzione con valori letterali e variabili che esprimano la risposta del prodotto di terze parti.
- Un operatore di calcolo Failure per la mappatura della stringa Process:FaultString alla corretta variabile di risposta di SOAP.

Se il processo di destinazione di IT PAM riguarda un prodotto di assistenza tecnica di terze parti, verificare che il processo comprenda anche i seguenti elementi:

- L'operatore specifico del prodotto.

  Ad esempio, un processo che ha come destinazione il modulo BMC Remedy sarà definito con l'operatore Create_Help_Desk_Case.

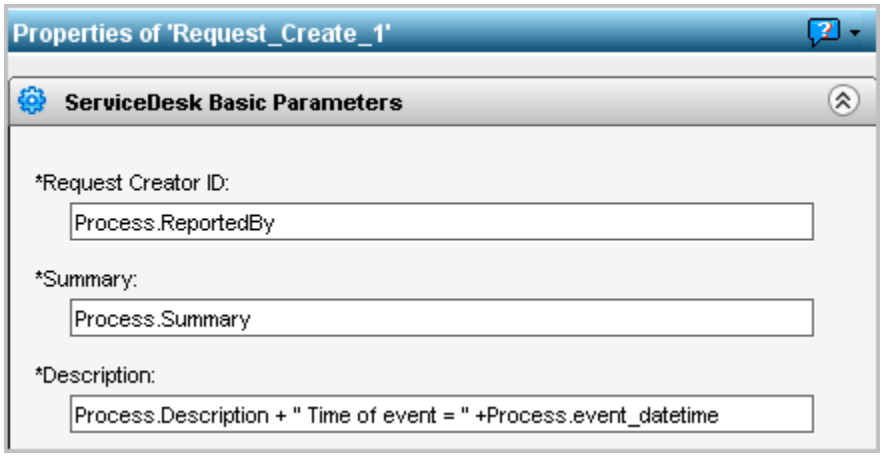
- I parametri specifici del prodotto associati ai parametri locali di processo: ReportedBy, Summary, Description, EndUser, Priority e Severity.

  Ad esempio, un processo che ha come destinazione il modulo BMC Remedy mapperà i parametri locali ai parametri HelpDesk Create Case.

Di solito, un processo di CA IT PAM comprende solo i parametri di processo predefiniti, ognuno dei quali viene mappato a un campo nel prodotto di terze parti. Se lo si desidera, è possibile aggiungere campi CEG come parametri di un dato processo. Nell'esempio sono mostrati i seguenti campi CEG nel dataset:

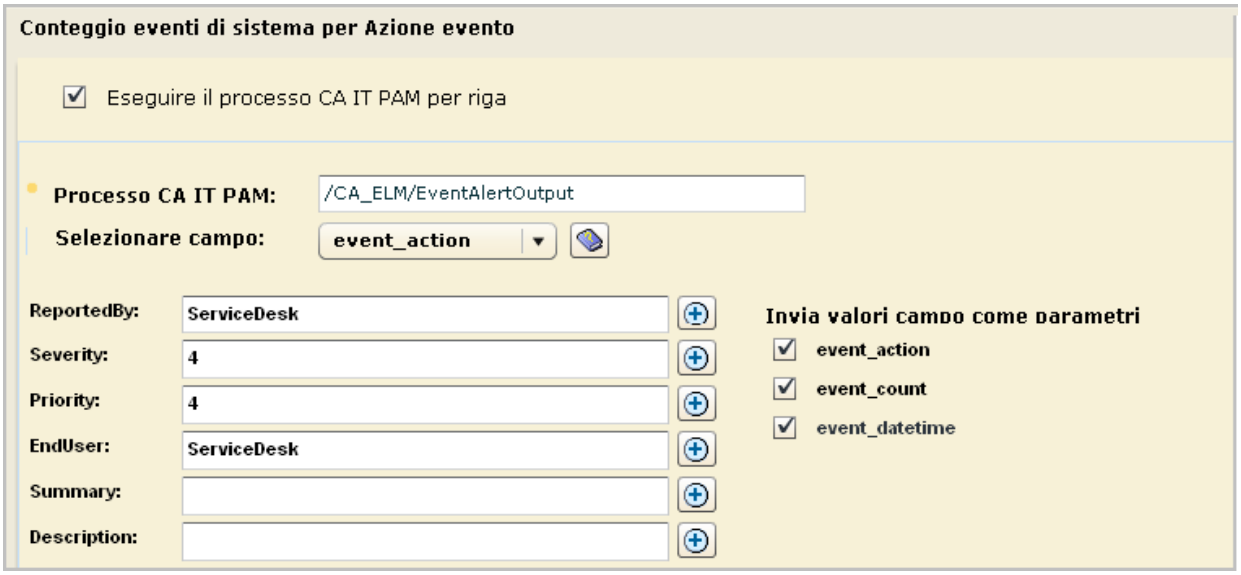
- event_severity
- event_count
- event_datetime

Ogni parametro di base viene mappato a un campo Service Desk. Ad esempio, il parametro di processo ReportedBy viene mappato al campo Assegnatario di CA Service Desk. Quando i campi CEG vengono aggiunti come parametri di processo, è possibile riferirsi ad essi in un parametro di base come valori. Ad esempio, è possibile definire il valore del campo CEG event_datetime in modo da poterlo visualizzare per impostazione predefinita nel campo Descrizione di CA Service Desk. È possibile eseguire tale operazione aggiungendo Process.event_datetime nel campo Descrizione dei parametri di base di Service Desk.

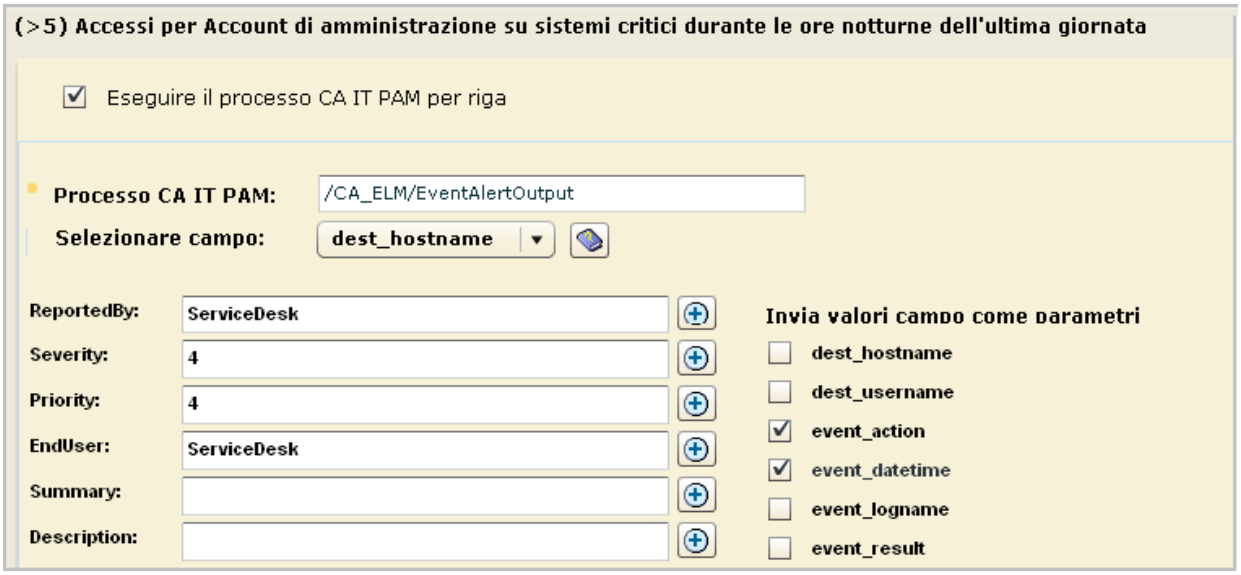


Quando si crea un avviso che esegua tale processo, esaminare i campi CEG elencati sotto Invia valori campo come parametri. Se uno o più parametri in elenco è un campo CEG che è stato definito come parametro di processo, selezionare tale campo. Considerare gli esempi riportati di seguito:

- Tutti e tre i campi CEG definiti nel dataset verranno visualizzati per la query Conteggio eventi di sistema per Azione evento. Pertanto, tutti e tre dovranno essere selezionati per inviarli come parametri a CA IT PAM.



- Due dei tre campi CEG definiti nel dataset verranno visualizzati per la query >5 accessi per account di amministrazione. Pertanto, sarà necessario selezionarli entrambi per inviarli come parametri a CA IT PAM.



Ulteriori informazioni:

Visualizzare il processo di output di evento/avviso campione (a pagina 396)

Raccogliere informazioni per l'integrazione di CA IT PAM

La maggior parte delle informazioni richieste per l'integrazione di CA IT PAM riguarda la configurazione del prodotto e dei relativi processi. È possibile avviare CA IT PAM e ricercare le informazioni di configurazione necessarie, oppure raccogliere le informazioni, registrarle e configurare rapidamente CA IT PAM inserendo i valori registrati.

È possibile fare riferimento sia ai processi campione importati sia ai processi personalizzati, modificati in base ai requisiti di CA User Activity Reporting Module.

Per raccogliere informazioni per l'integrazione di CA IT PAM

1. Accedere al server CA IT PAM locale e verificare che si tratti di CA IT Process Automation Manager 2.1.
2. Fare clic sul collegamento al client ITPAM.
3. Raccogliere le informazioni relative ai primi quattro campi della configurazione di CA IT PAM.
   a. Fare clic su Browser di configurazione.
   b. Fare clic sulla scheda Proprietà.
   c. Registrare il valore di nome server come proprio valore per il server di CA IT PAM.
   d. Accettare la porta 8080 per CA IT PAM.
   e. Richiedere le credenziali per l'accesso a CA User Activity Reporting Module all'amministratore di CA IT PAM e registrarle come nome utente e password.

Campo per la configurazione di CA IT PAM	Descrizione	Il proprio valore
Server CA IT PAM	Nome di host completo del server su cui è installato CA IT PAM. Tale valore verrà visualizzato nel campo Nome server della scheda Proprietà del Browser di configurazione.	
Porta di CA IT PAM	La porta predefinita è 8080 Tale valore verrà visualizzato nel campo URL di dominio della scheda Proprietà del Browser di configurazione.	8080
Nome utente	ID utente utilizzato da CA User Activity Reporting Module per accedere a CA IT PAM ed eseguire un processo. Richiederlo all'amministratore di CA IT PAM Esempio: itpamadmin	
Password	Password associata al nome utente Richiederla all'amministratore di CA IT PAM.	

4. Registrare il percorso ed il nome dei processi che si prevede di eseguire da CA User Activity Reporting Module.
   a. Dal menu File del client ITPAM, selezionare Apri browser di libreria
   b. Nella scheda Cartelle, selezionare la cartella della libreria contenente il processo di output di evento/avviso.
   c. Registrare il percorso ed il nome del processo di output di evento/avviso.
   d. Se diversa, selezionare la cartella di libreria contenente il processo che restituisce i valori correnti di una chiave specifica.
   e. Registrare il percorso ed il nome del Processo valori dinamici.

Campo specifico di processo CA IT PAM	Descrizione ed esempio	Il proprio valore
Processo di output di evento/avviso	Percorso e nome del processo. Identifica il processo il cui scopo è inviare ad un prodotto esterno come CA Service Desk i dettagli configurati con l'avviso o un URL. Esempio: /CA_ELM/EventAlertOutput	
Processo valori dinamici	Percorso e nome del processo. Identifica il processo il cui scopo è raccogliere i valori della chiave di input e restituirli per l'analisi in un file csv. Esempio: /CA_ELM/ValuesList	

5. Raccoglie i parametri del processo di output di evento/avviso:
   a. Per aprire il processo, fare doppio clic sul processo di output di evento/avviso a cui si è fatto riferimento.
   b. Nella scheda Editor principale, fare clic sull'icona Request_Create per visualizzare le proprietà.
   c. Visualizzare i parametri di base di ServiceDesk
   d. Nella prima colonna sottostante, registrare i parametri preceduti da Processo: se non corrispondono esattamente a quanto viene visualizzato
   e. Fare clic sulla scheda Dataset.
   f. Fare clic su ogni parametro di Local_Dataset e registrarne il valore predefinito, se esistente.

Parametri del processo di output di evento/avviso	**Descrizione ed esempio**	**Il proprio valore**
ReportedBy	Nome utente ServiceDesk valido.	
Riepilogo	Questo testo viene visualizzato nel campo Riepilogo della richiesta Service Desk. Ad esempio, “Richiesta creata da CA ELM”	---
Descrizione	Questo testo viene visualizzato nel campo Descrizione della richiesta Service Desk.	---
EndUser	Nome utente ServiceDesk valido.	
Priorità	Imposta la priorità predefinita. Se non è configurato alcun valore predefinito, registrare un valore compreso tra 1 e 5. Esempio: 3	
Gravità	Imposta il livello di gravità predefinito. Se non è configurato alcun valore predefinito, registrare un valore compreso tra 1 e 5. Esempio: 4	

Esempio: eseguire un processo di output di evento/avviso con i risultati della query selezionata

Tutti gli utenti sono autorizzati ad eseguire su richiesta un processo di CA IT PAM. È possibile eseguire il processo di output di evento/avviso di CA IT PAM configurato con i risultati della query selezionata per ognuno dei seguenti scopi:

- Per eseguire un processo di output di evento/avviso su richiesta in base alle necessità attuali.
- Per testare i risultati di elaborazione prima di creare un avviso pianificato per la query in questione, utilizzando come destinazione il processo di CA IT PAM.

È possibile eseguire un processo di CA IT PAM da una riga di risultati della query visualizzati. Ciò presume che i risultati siano visualizzati come tabella, anziché come diagramma. Le righe dei risultati della query possono essere visualizzate in uno dei seguenti modi:

- Dall'elenco delle query, selezionare una query che restituisca risultati.
- Selezionare un rapporto dall'elenco dei rapporti e selezionare una query che restituisca risultati.
- Inserire un prompt che restituisca risultati.

Nota: il seguente argomento presume che una riga di risultati di una query venga visualizzata una volta selezionata la query dal relativo elenco.

Per conoscere i dati restituiti per i campi della CEG, consultare l'argomento *Grammatica evento comune (CEG)* nella Guida in linea.

Per eseguire manualmente il processo di CA IT PAM configurato in base a una riga di risultati della query visualizzata

1. Fare clic sulla scheda Query e rapporti e sulla sottoscheda Query.

   Verranno visualizzati l'elenco Filtro tag query e l'Elenco query.

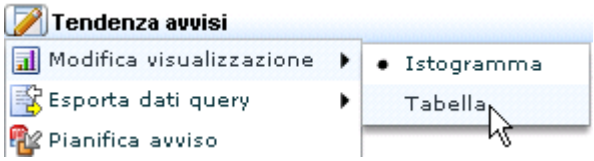
2. (Facoltativo) Inserire i criteri di ricerca nell'elenco delle query, ad esempio gli account predefiniti.

   Gli eventi corrispondenti agli accessi effettuati dagli account predefiniti sono soggetti all'inoltro al processo di output di evento/avviso di CA IT PAM.

3. Dall'elenco delle query, selezionare la query di cui si desidera visualizzare i risultati.

   In alternativa, è possibile visualizzare la sottoscheda Rapporti, selezionare un'opzione dall'Elenco rapporti, passare alla visualizzazione delle singole query e selezionarne una.

4. Se i risultati vengono visualizzati in un diagramma, selezionare Modifica visualizzazione dall'elenco a discesa dei nome delle query e scegliere Tabella.



5. Selezionare la riga dei risultati della query per cui eseguire il processo di CA IT PAM.

6. Fare clic col tasto destro del mouse su questa riga di risultati di query, e selezionare Eseguire il processo CA IT PAM dall'elenco a discesa.

Verrà visualizzata la finestra di dialogo Eseguire il processo CA IT PAM. Tale finestra contiene il nome ed i parametri di processo definiti nella configurazione di IT PAM del servizio di server dei rapporti. Inoltre, nella stessa finestra l'elenco a discesa Selezionare campo consente di inserire dati variabili restituiti al campo della CEG selezionato.

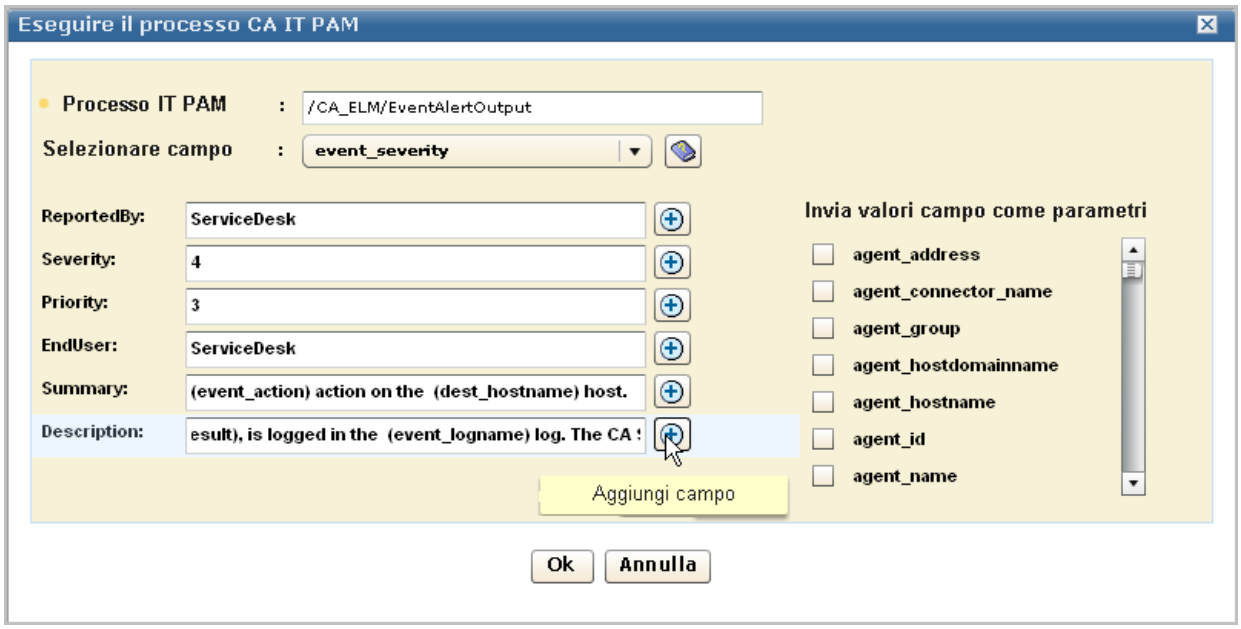
7. Compilare i campi nel modo seguente:
   a. Controllare i valori predefiniti per i parametri di processo visualizzati ed identificare eventualmente quelli da modificare.

      Questi parametri ed i valori relativi derivano dalla configurazione dell'integrazione di CA IT PAM.
   b. Per modificare il valore predefinito visualizzato, inserirne un nuovo valore.
   c. Per specificare un valore variabile, selezionare il relativo campo della CEG dall'elenco a discesa Selezionare campo, nella parte superiore della finestra di dialogo, quindi fare clic su Aggiungi campo, accanto alla relativa casella di testo.
   d. Per ogni campo vuoto, inserire un valore, selezionare una variabile ed aggiungerla oppure digitare una frase che comprenda le variabili selezionate.

      Riepilogo esemplificativo: in (event_datetime), l'account (dest_username) ha eseguito un'azione (event_action) sull'host (dest_hostname).

      Descrizione esemplificativa: il risultato dell'azione (event_result) è registrato in (event_logname). Il livello di gravità CA è (event_severity).
   e. Se il processo di CA IT PAM specifica parametri riferiti a campi della CEG aggiuntivi, selezionare questi ultimi dall'elenco visualizzato per l'invio come parametri.

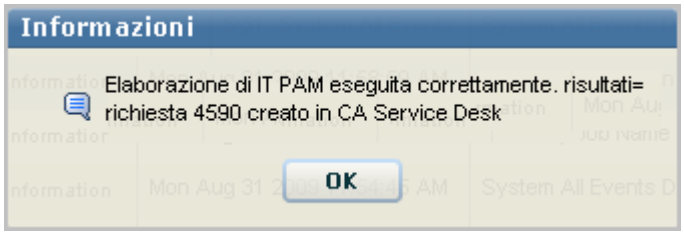
   Segue un esempio: La visualizzazione in uso potrebbe contenere altri campi definiti nel processo di output di evento/avviso di IT PAM personalizzato.



8. Fare clic su OK.

   Verrà visualizzata la finestra di avanzamento, seguita da un messaggio che indica l'esito dell'esecuzione del processo di CA IT PAM e, in caso di esito positivo, i relativi risultati.

   Segue un esempio in cui il risultato è la richiesta 4590 creata in Service Desk.



9. Fare clic su OK.

10. Per visualizzare i risultati in CA Service Desk, accedere e ricercare la richiesta contrassegnata dal numero presente nel messaggio.

    Ad esempio, selezionare Richiesta ed inserire 4590.

11. Verranno visualizzati risultati di Service Desk simili ai seguenti.

12. Confrontare il riepilogo ed i dati di descrizione pianificati, definiti al passaggio 7, con quelli visualizzati nelle informazioni di riepilogo. Essi comprendono i dati relativi al livello di gravità CA.

Progettare le query di eventi da inviare al processo di output di evento/avviso

Una volta configurata l'integrazione di CA IT PAM, è possibile iniziare a pianificare gli avvisi che generano l'output di evento/avviso, compilando un elenco di query su cui basare tali avvisi. Solitamente, si tratta di query relative ad eventi di violazione dei criteri. È possibile adottare una combinazione di svariati approcci:

- Analizzare gli avvisi attualmente pianificati per identificare quelli che devono eseguire il processo di output di evento/avviso. Per esempio, se il processo di output di evento/avviso invia una notifica ad un'applicazione help desk, è possibile identificare gli avvisi che apriranno un ticket dell'help desk.
- Analizzare i criteri in uso per identificare quelli la cui violazione può risalire ad un evento registrato, quindi creare una query per questo tipo di evento.
- Esaminare i risultati delle altre query predefinite per identificare i dati utilizzabili da un prodotto di terze parti, ad esempio un prodotto help desk, per eseguire un'azione correttiva.
- Se il processo di output di evento/avviso di CA IT PAM crea ticket in un prodotto help desk di terze parti, controllare i tipi di ticket dell'help desk più comuni in modo da individuare le cause che potrebbero essere acquisite come registri di evento.

Per identificare o progettare le query su cui basare gli avvisi che eseguono i processi di output di evento/avviso di CA IT PAM

1. Per ogni tipo di evento che richieda un ticket dell'help desk, identificare, modificare o creare una o più query in grado di acquisire i dati relativi all'evento in questione.
   - Identificare ogni query predefinita in grado di raccogliere eventi in base a tali condizioni.
   - Se occorre personalizzare una query predefinita, eseguirne una copia e modificarla in base alle proprie esigenze.
   - Se non esiste una query predefinita in grado di raccogliere un determinato tipo di eventi che richiedano una notifica dell'help desk, creare la query o le query necessarie.
2. Per ogni query finalizzata alla ricerca di eventi IT in cui uno dei campi può assumere uno fra diversi valori noti, utilizzare un elenco con chiave predefinito, personalizzarlo o crearne uno nuovo. Se i valori di questo tipo di chiave si trovano in un file csv, importare il file. Per un elenco generato da un processo di IT PAM, configurare quest'ultimo come processo di valori dinamici, creare la chiave ed importare i valori da CA IT PAM.
3. Stabilire se eseguire il processo di output di evento/avviso di CA IT PAM per ogni query che restituisca risultati o per ogni riga di risultati.
4. Eseguire il test della query.
   a. Creare le condizioni che generano l'evento da acquisire.
   b. Eseguire manualmente la query o il set di query
   c. Valutare se i risultati della query siano sufficienti al personale dell'help desk per completare il follow-up necessario.
   d. In caso contrario, modificare la query o il set di query in modo da fornire le informazioni necessarie, ed eseguire nuovamente il test.

Questa preparazione garantisce che, al momento di pianificare un avviso che esegue ogni query o set di query di questo tipo, l'output di evento/avviso risultante conterrà i dati necessari per la risoluzione.

Ulteriori informazioni:

Personalizzare le query per gli avvisi (a pagina 370)

Esempio: inviare un avviso che esegue un processo IT PAM per riga

È possibile inviare un avviso che esegue il processo CA IT PAM di output di evento/avviso per riga o per query. Questo esempio illustra la procedura di esecuzione del processo per riga. Esso comprende un esempio di ciò che può essere visualizzato per questo tipo di avviso dal personale che utilizza sia CA IT PAM che il prodotto di terze parti a cui CA IT PAM invia le informazioni.

Prima di creare un avviso per eseguire un processo IT PAM per una determinata query, si consiglia di identificare le colonne CEG che restituiscono dati. Tali colonne devono essere selezionate al momento della creazione di un'istruzione di riepilogo e descrizione per l'avviso.

Nota: copiare la query e fare clic sul passaggio Colonne query. Per i campi progettati per essere visibili, individuare il nome di colonna corrispondente al nome visualizzato. Ad esempio, il campo CEG utilizzato per compilare la colonna Account è dest_username.

Colonne selezionate

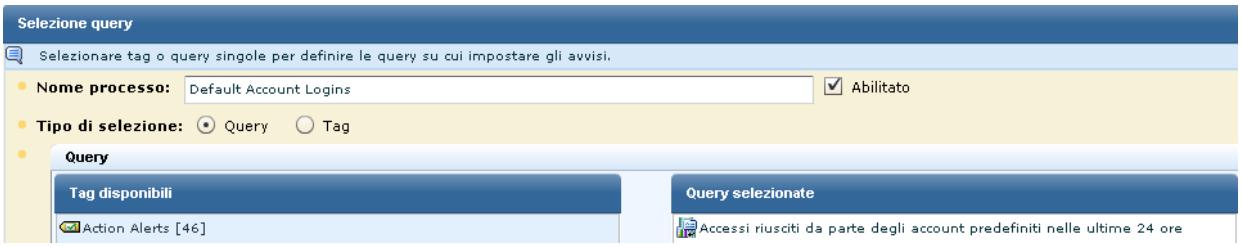
Visualizza nome	Colonne	Visibile
Date	event_datetime	☑
Account	dest_username	☑
Host	dest_hostname	☑
Log Name	event_logname	☑
Action	event_action	☑
Result	event_result	☑

Per creare un avviso quando un membro di un account predefinito esegue correttamente l'accesso

1. Fare clic sulla scheda Gestione avvisi e quindi sulla sottoscheda Pianificazione avvisi.
2. Fare clic su Pianifica un avviso.

   Viene visualizzata la procedura guidata di pianificazione avvisi.

3. Completare il passaggio Selezione avviso come segue:
   a. Inserire il nome del processo, ad esempio Accessi degli account predefiniti.
   b. Fare clic sul tag Avvisi.
   c. Selezionare la query Accessi riusciti da parte degli account predefiniti nelle ultime 24 ore e spostarla nell'elenco Query selezionate.



4. Selezionare un intervallo di data per l'esecuzione della query e il numero massimo di righe da visualizzare.
   a. Fare clic su Condizioni risultato.
   b. Selezionare un intervallo di data, come ad esempio "adesso" e "adesso" "-1 ore"
   c. Selezionare come event_datetime parametri di visualizzazione dei risultato come il limite di righe pari a 10 e la granularità tempo.
   d. Ignorare gli eventi raggruppati.
5. Definire la pianificazione.
6. Definire i dati di avviso da trasmettere al processo CA IT PAM, insieme ai dati di evento recuperati dalla query.
   a. Fare clic sul passaggio Destinazione.
   b. Selezionare la scheda Processo CA IT PAM.
   c. Selezionare Accessi riusciti da parte degli account predefiniti nelle ultime 24 ore.
   d. Selezionare Eseguire il processo CA IT PAM per riga.
   e. Se il processo CA IT PAM configurato non è quello che si desidera eseguire, modificare il percorso ad esso relativo. Il processo CA IT PAM deve contenere il percorso completo preceduto dal carattere /.

f. (Facoltativo) Creare un'istruzione di riepilogo con testo letterale e variabili. Le variabili sono ricavate dai campi della CEG al momento del perfezionamento dei dati raccolti per una riga. Segue un esempio di istruzione di riepilogo che utilizza le variabili.

```
L'account (dest_username) ha eseguito l'azione (event_action) su
(dest_hostname)
```

La prima istruzione si crea come segue:

- Digitare la parola "L'"
- Selezionare dest_username dall'elenco a discesa Selezionare campo e fare clic sulla casella + accanto al campo Riepilogo.
- Digitare la frase "account ha eseguito l'"
- Selezionare event_action dall'elenco a discesa Selezionare campo e fare clic sulla casella + accanto al campo Riepilogo.
- Digitare la frase "azione su"
- Selezionare dest_hostname dall'elenco a discesa Selezionare campo e fare clic sulla casella di controllo + accanto al campo Riepilogo.

g. (Facoltativo) Creare una descrizione con testo letterale e testo derivato dei campi CEG. Selezionare il campo desiderato nell'elenco a discesa Selezionare campo e fare clic sulla casella +. Ad esempio:

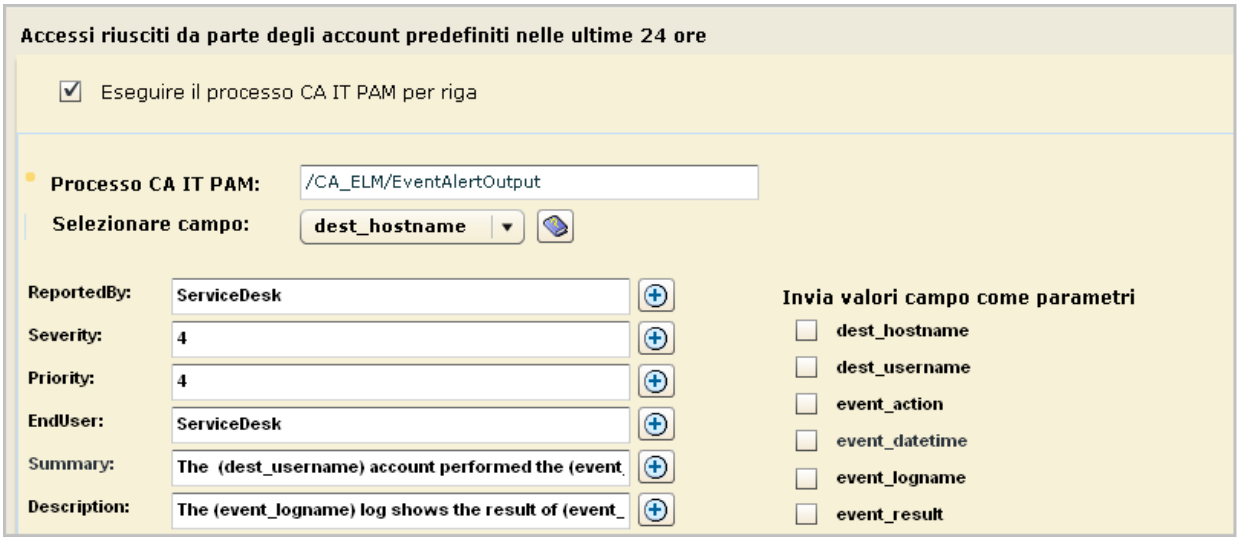
```
Il registro (event_logname) visualizza il risultato di (event_result) su
(event_datetime)
```

```
Il risultato (event_result) di (event_action) viene inserito nel registro
(event_logname).
```

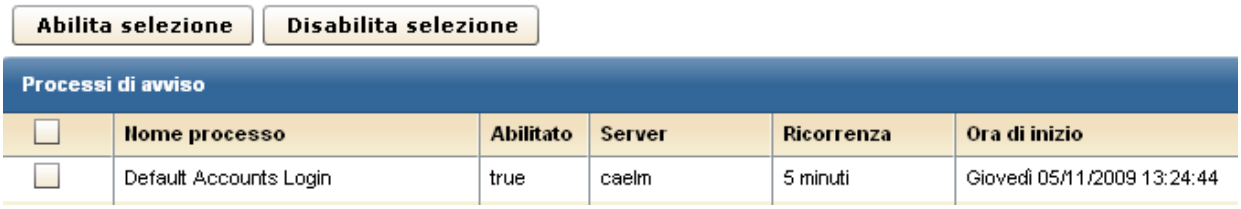
```
Il registro (event_logname) visualizza l'azione (event_action) il cui
risultato è (event_result).
```

h. Per Invia valori campo come parametri, selezionare ogni campo CEG utilizzato come parametro di processo dal processo IT PAM specificato.

Nota: poiché il processo selezionato non utilizza nomi di campo CEG come parametri, in questo esempio non verrà selezionato nessun campo. Per stabilire se un processo personalizzato utilizza questo tipo di parametri, visualizzare la scheda Dataset nel processo CA IT PAM di output di evento/avviso.



7. Selezionare un server.
8. Fare clic su Salva e chiudi.
   Il processo verrà visualizzato nell'elenco Processi di avviso.



9. Per visualizzare i risultati, fare clic su Gestione avvisi, Eventi di automonitoraggio. Verrà visualizzata una visualizzazione parziale delle righe di informazioni:

Azione	Risultato	Descrizione risultato
Resource Modify	S	Update RSSFeed Alert Name [login attempts] on reportServer [ca-elm] recurrence [5] recurrenceType [Minutes] was Successful.
Alert Creation	S	Alert job [Default Account Logins] created successfully.
Alert Job Setup	S	Schedule Action Query Alert Name [Default Account Logins] on reportServer [ca-elm] was Successful.

10. Fare clic sulla scheda Gestione avvisi, quindi sulla sottoscheda Avvisi. Selezionare l'avviso pianificato per visualizzare i risultati della query.

Nome avviso	Categoria	Data
Default Account Logins	Accessi riusciti da parte degli account predefiniti nelle ultime 24 ore	Giovedì 12/11/2009 16:09:28

Default Account Logins

Alert name(Default Account Logins) Alert created by(su) Federated job(Yes) Tags (Action Alerts) Time Zone (America/New_York) Reports on successful login activity by user accounts listed in Default_Accounts keyed list during the last 24 hour time frame Rows Returned(1)

Data	Account	Host	Nome log	Azione	Risultato
Giovedì 12/11/2009 16:09:28	su	ca-elm	CALM	Login Attempt	S

11. Osservare i risultati restituiti da CA IT PAM nella scheda eventi di automonitoraggio.

    Segue un parziale esempio di messaggio di conferma, in cui il messaggio viene visualizzato negli eventi di automonitoraggio del server di rapporto. Notare il numero di ticket che segue Risultati =.

Azione	Risultato	Descrizione risultato
Notification Creation	S	IT PAM process ran successfully. Results = [Request 631 created in CA Service Desk.]

12. (Facoltativo) Controllare i risultati su CA Service Desk come segue:
    a. Accedere a CA Service Desk.
    b. Selezionare Richiesta ed inserire il numero della richiesta.
    c. Fare clic sul collegamento relativo al numero della richiesta per controllare i dettagli sul problema e le informazioni di riepilogo.

Ulteriori informazioni:

Linee guida per la creazione di un processo di output di evento/avviso (a pagina 401)

Esempio: inviare un avviso che esegua un processo di IT PAM per query

È possibile inviare un avviso che esegue il processo di output di evento/avviso di CA IT PAM per riga o per query. Questo esempio illustra la procedura di esecuzione del processo per query. Esso comprende un esempio di ciò che può essere visualizzato per questo tipo di avviso dal personale autorizzato che lavora con il prodotto di terze parti a cui CA IT PAM ha inviato le informazioni.

Per inviare un avviso che esegue il processo di output di evento/avviso di CA IT PAM per query

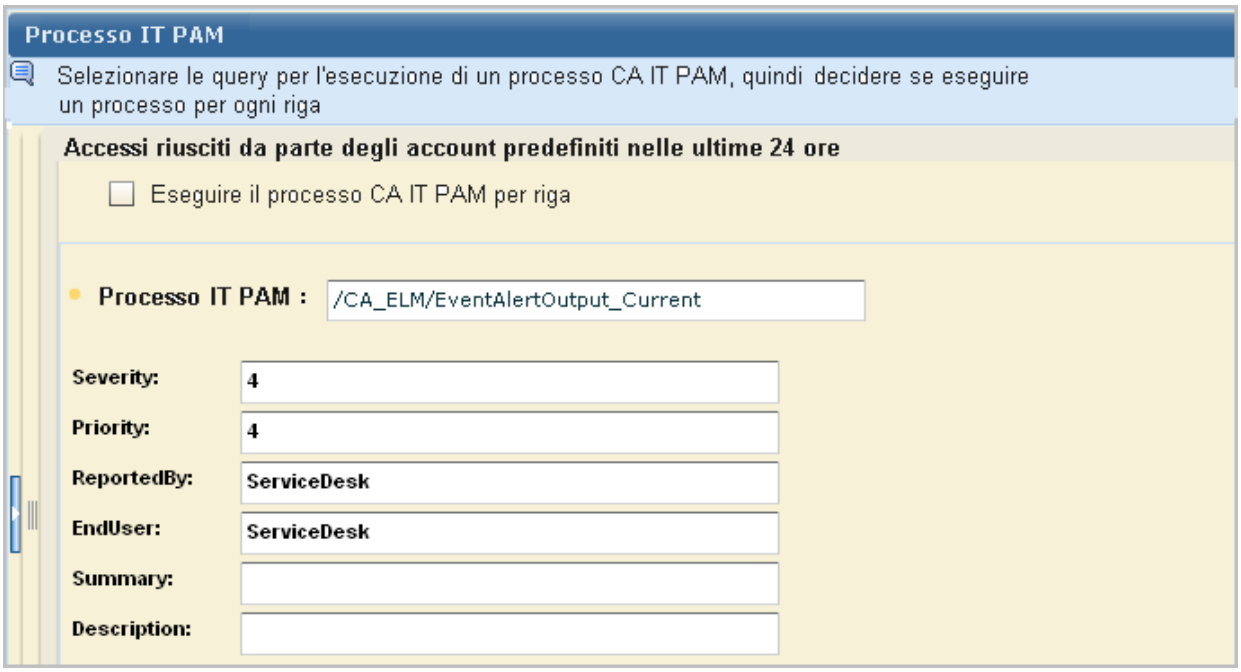
1. Fare clic sulla scheda Gestione avvisi e quindi sulla sottoscheda Pianificazione avvisi.
2. Fare clic su Pianifica un avviso.

   Viene visualizzata la procedura guidata di pianificazione avvisi.
3. Completare il passaggio Selezione avviso come segue:
   a. Immettere il nome del processo.
   b. Selezionare una query.
4. (Facoltativo) Selezionare un intervallo di data per l'esecuzione della query e il numero massimo di righe da visualizzare.
   a. Fare clic su Condizioni risultato.
   b. Selezionare un intervallo di data, come ad esempio "adesso" e "adesso" "-1 ore"
   c. Selezionare i parametri di visualizzazione del risultato.
5. Definire la pianificazione.
6. Definire i dati di avviso da inviare al processo CA IT PAM, insieme ai dati di evento recuperati dalla query.
   a. Fare clic sul passaggio Destinazione.
   b. Selezionare la scheda Processo CA IT PAM.
   c. Selezionare la query da inviare

   Accessi riusciti da parte degli account predefiniti nelle ultime 24 ore

d. Per ottenere un rapporto dei risultati per query, lasciare vuoto Eseguire il processo CA IT PAM per riga.

e. Facoltativamente, digitare il testo letterale nei campi di Riepilogo e Descrizione.



7. Selezionare un server.

8. Fare clic su Salva e chiudi.
   Il processo verrà visualizzato nell'elenco Processi di avviso.

9. Fare clic sulla scheda Gestione avvisi, quindi sulla sottoscheda Avvisi. Selezionare l'avviso pianificato per visualizzare i risultati della query.

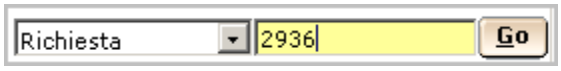
10. Fare clic sulla scheda dell'evento di automonitoraggio per l'azione Creazione notifica con i risultati restituiti da CA IT PAM. Il messaggio di conferma conterrà il numero di richiesta creato nell'applicazione di terze parti, a patto che si tratti di un prodotto help desk.

Azione	Risultato	Descrizione risultato
Notification Creation	S	IT PAM process ran successfully. Results = Request 2936 created in CA Service Desk.

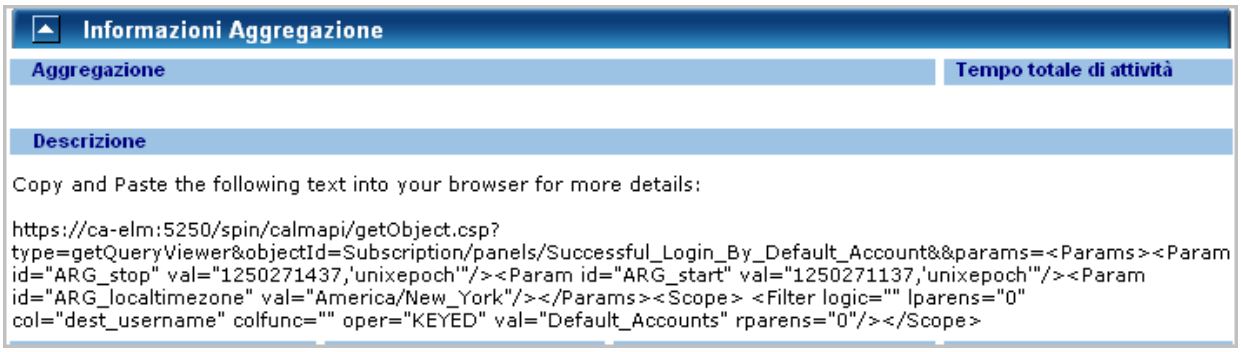
11. (Facoltativo) Per visualizzare ciò che vede il personale dell'help desk, controllare i risultati su CA Service Desk come segue:

    a. Accedere a CA Service Desk.

    b. Selezionare Richiesta ed inserire il numero visualizzato nella descrizione del risultato di Creazione notifica. Fare clic su Vai a.



    c. Copiare l'URL visualizzato nella sezione Informazioni di riepilogo ed incollarlo nel browser.



Verrà visualizzata la finestra di accesso a CA User Activity Reporting Module.

    d. Accedere a CA User Activity Reporting Module. È possibile utilizzare un account con un ruolo dotato di privilegi ridotti, ad esempio Revisore.

    I dati di evento restituiti dalla query verranno presentati sottoforma di visualizzazione predefinita della query, vale a dire come tabella o come diagramma.

Se la visualizzazione è in formato tabella, è possibile visualizzare i dati degli eventi non elaborati.

Ulteriori informazioni:

Impostare le destinazioni di notifica (a pagina 474)

Modalità di utilizzo delle trap SNMP

In generale, i sistemi di gestione degli errori ed i centri delle operazioni di rete (NOC) sono abilitati per il ricevimento di trap SNMP. A seconda del prodotto di destinazione, è possibile inviare avvisi a tali sistemi sotto forma di trap SNMP v2 o v3.

Di seguito vengono riportate le attività richieste per l'utilizzo di trap SNMP:

- Creazione di MIB personalizzata per ogni avviso destinato a CA NSM.
- Preparazione di prodotti di destinazione per la ricezione di trap SNMP da CA User Activity Reporting Module.
- Pianificazione di avvisi con una o più destinazioni di trap SNMP.

La configurazione della destinazione di trap SNMP predefinita è facoltativa.

Informazioni sui trap SNMP

SNMP è l'acronimo di Simple Network Management Protocol (Protocollo semplice di gestione di rete), uno standard aperto per inviare messaggi di avviso ad una specifica destinazione. Esistono tre versioni di SNMP: SNMP v1, SNMP v2 e SNMP v3. CA User Activity Reporting Module consente di utilizzare entrambe le versioni SNMP v2 e v3 per inviare un avviso a uno o più sistemi di gestione di terze parti quando si verifica un evento che genera un avviso.

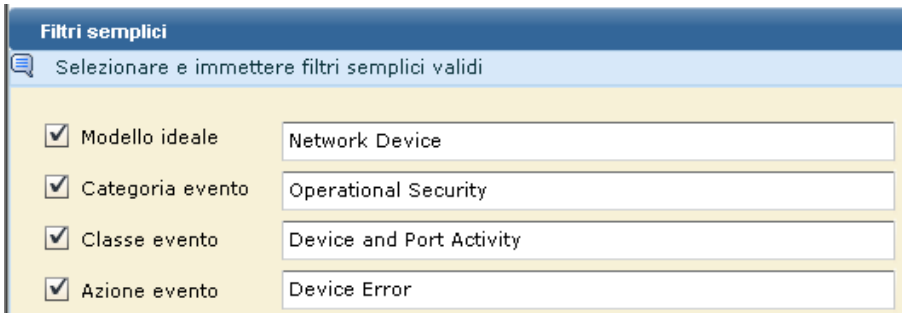
In CA User Activity Reporting Module verrà generato un avviso quando una query pianificata restituisce dal database del registro eventi i risultati degli eventi perfezionati di recente. È possibile configurare una query pianificata usando un trap SNMP come destinazione. I ricevitori di trap, ovvero i sistemi gestionali di destinazione, sono in grado di elaborare fino a circa 200 trap al secondo. In genere, i ricevitori di trap sono in ascolto sulla porta UDP 162, quella di snmptrap.

CA User Activity Reporting Module consente di creare in maniera versatile avvisi personalizzati da inviare come trap SNMP. Ad esempio, è possibile definire avvisi che inviino una notifica dell'occorrenza di un evento critico. È anche possibile definire avvisi per eventi come le modifiche di configurazione e decidere quali avvisi inviare come trap SNMP.

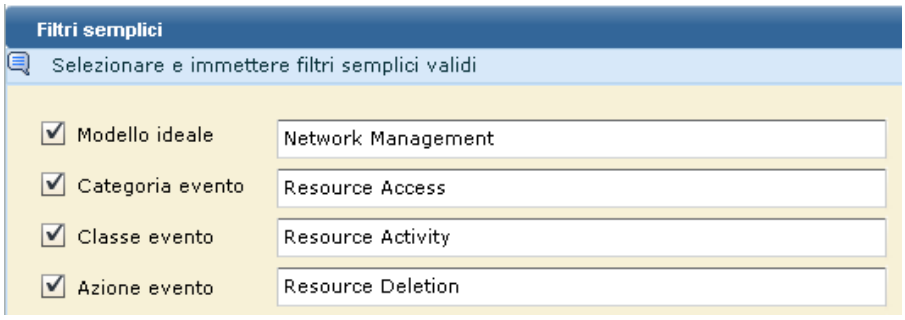
Esempi di filtri semplici per gli avvisi da inviare come trap

Gli eventi con impatti negativi sulle operazioni (ad esempio, arresto dei servizi, errori nei dispositivi ed eliminazione delle risorse) sono rilevanti per i centri delle operazioni di rete (NOC, Network Operations Center). È possibile generare avvisi quando tali eventi si verificano ed indirizzarli verso il proprio NOC. A tal proposito, è possibile creare avvisi personalizzati tramite filtri semplici in una query personalizzata. Considerare i seguenti esempi di filtro semplice.

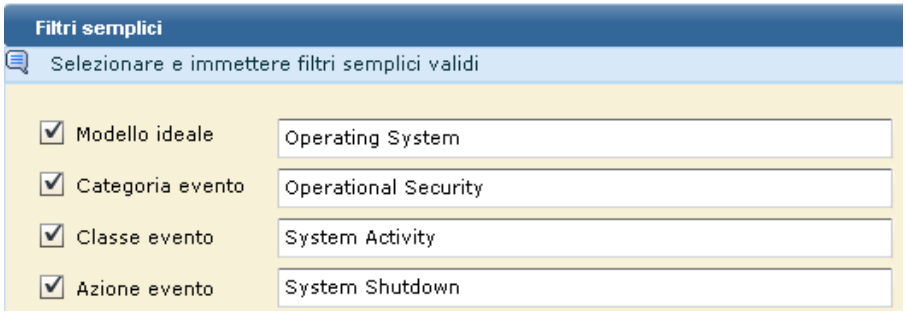
- Errore dispositivo



- Eliminazione risorsa



- Arresto del sistema



Informazioni sui file MIB

I trap SNMP vengono definiti sia nei file MIB (Management Information Base, base di informazioni di gestione) standard che in quelli specifici dell'azienda.

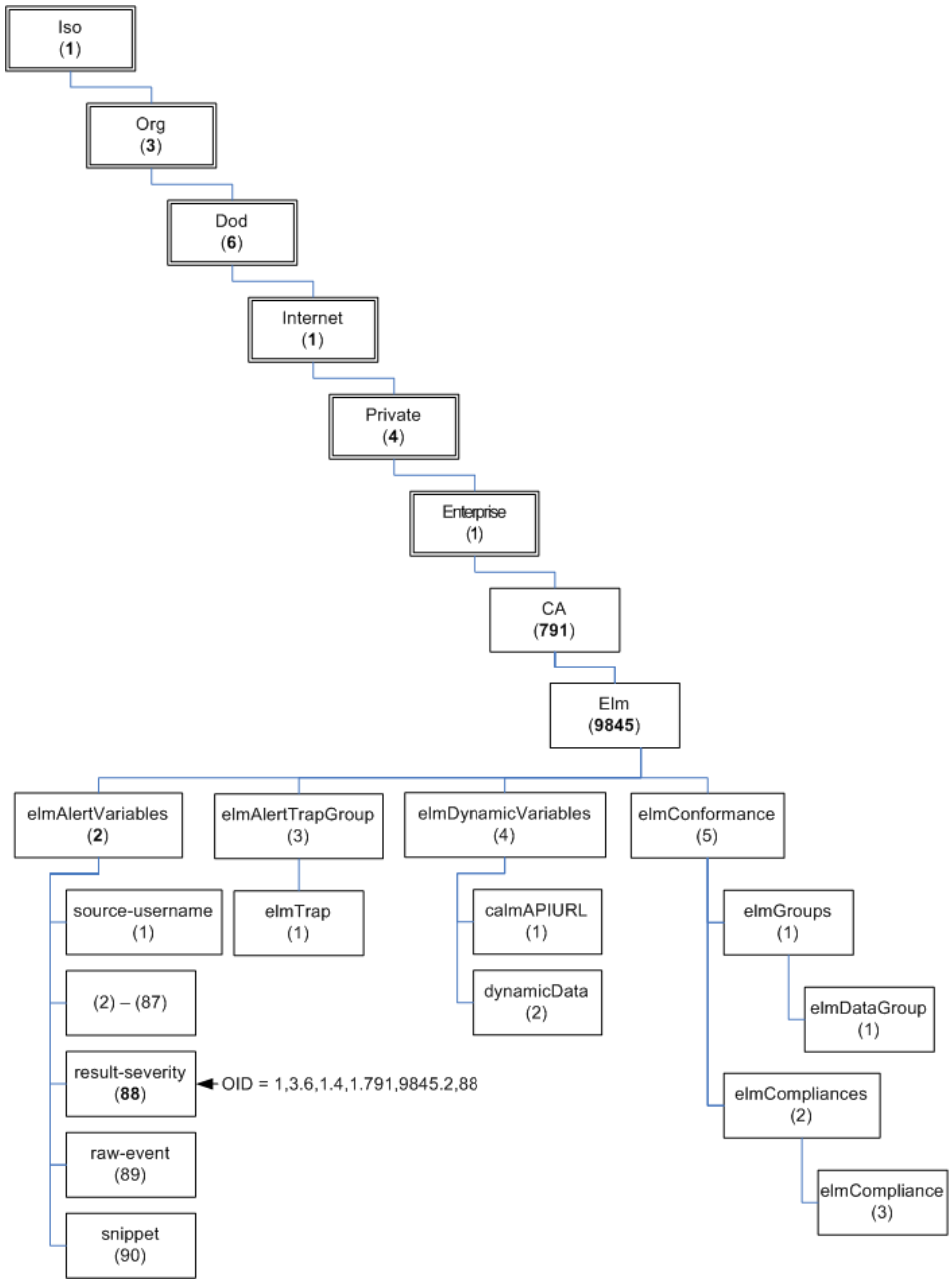
Ogni azienda privata sull'albero MIB utilizza un numero univoco preceduto dai numeri dei relativi nodi padre. ICANN ha assegnato a CA, Inc. il numero privato di azienda 791. I dati inviati da ogni applicazione CA nei trap SNMP saranno associati a ID di oggetto che iniziano con 1.3.6.1.4.1.791. L'applicazione CA User Activity Reporting Module appartenente a CA dispone dell'identificatore 9845. Tutti i dati di trap SNMP inviati dagli avvisi di CA User Activity Reporting Module verranno associati a ID di oggetto (OID) che iniziano con 1.3.6.1.4.1.791.9845.

CA User Activity Reporting Module fornisce un solo file MIB. Il nome di questo MIB è CA-ELM.MIB. Questo MIB definisce tutti i campi che possono essere inviati dagli avvisi con un unico trap. Tale trap comprende tutti i campi di CEG disponibili in CA User Activity Reporting Module.

Quando l'avviso viene inviato ad una destinazione di trap SNMP, i dati inviati comprendono un URL. I singoli trap di monitoraggio in arrivo possono esplorare l'URL inviato dall'avviso. Esplorando l'URL verrà aperta una pagina di CA User Activity Reporting Module che contiene i risultati di query in un formato semplice da leggere. Questa funzionalità rende inutile l'utilizzo dei MIB per interpretare i dati inviati come trap SNMP.

Struttura MIB di CA-ELM

È possibile visualizzare la struttura del file CA-ELM.MIB nel formato di struttura MIB. I campi CEG vengono definiti in elmAlertVariables con identificatori di oggetto SNMP univoci. Ad esempio, l'OID di result_severity è 1.3.6.1.4.1.791.9845.2.88.



File CA-ELM.MIB

Il file MIB di CA User Activity Reporting Module, CA-ELM.MIB, si trova sul DVD di installazione. La MIB di CA User Activity Reporting Module viene generata dal documento CEG di origine, che contiene gli OID per ogni campo CEG (elmAlertVariables).

Il file CA-ELM.MIB inizia con le importazioni, come riportato di seguito:

```
CAELM-MIB DEFINITIONS ::= BEGIN

  IMPORTS
        MODULE-IDENTITY, OBJECT-TYPE, Integer32, NOTIFICATION-TYPE
                FROM SNMPv2-SMI
        MODULE-COMPLIANCE, OBJECT-GROUP,NOTIFICATION-GROUP
                FROM SNMPv2-CONF                        DisplayString
                FROM SNMPv2-TC
```

La rappresentazione seguente è progettata per mostrare la struttura dell'albero della MIB di CA User Activity Reporting Module, dove i nodi principali comprendono iso(1) org(3) dod(6) internet(1) private(4) enterprises(1). Il formato del file CA-ELM.MIB corrente non corrisponde a quello della presente rappresentazione.

```
ca OBJECT IDENTIFIER::= { enterprises 791 }
        elm MODULE-IDENTITY...::= { ca 9845 }
                elmAlertVariables  ::= { elm 2 }
                        source-username    ::= { elmAlertVariables 1 }
                        source-domainname  ::= { elmAlertVariables 2 }
                        source-groupname   ::= { elmAlertVariables 3 }
                     ...
                        result-severity    ::= { elmAlertVariables 88 }
                        raw-event          ::= { elmAlertVariables 89 }
                        snippet            ::= { elmAlertVariables 90 }
                elmAlertTrapGroup  ::= { elm 3 }
                        elmTrap            ::= { elmAlertTrapGroup 1 }

                elmDynamicVariables    ::= { elm 4 }
                        calmAPIURL         ::= { elmDynamicVariables 1 }
                        dynamicData        ::= { elmDynamicVariables 2 }
                elmConformance         ::= { elm 5 }
                        elmGroups          ::= { elmConformance 1 }
                                elmDataGroup   ::= { elmGroups 1 }
                        elmCompliances     ::= { elmConformance 2 }
                                elmCompliance  ::= { elmCompliances 3 }
```

Il file CA-ELM.MIB definisce una trap. Tale trap viene definita nella maniera seguente:

```
elmTrap NOTIFICATION-TYPE
    OGGETTI {  source-username,source-domainname,source-groupname,source-
uid,source-gid,source-hostname,source-hostdomainname,source-address,source-mac-
address,source-port,source-processname,source-objectname,source-
objectattr,source-objectid,source-objectclass,source-objectvalue,dest-
username,dest-domainname,dest-groupname,dest-uid,dest-gid,dest-hostname,dest-
hostdomainname,dest-address,dest-mac-address,dest-port,dest-objectname,dest-
objectattr,dest-objectid,dest-objectclass,dest-objectvalue,agent-name,agent-
address,agent-hostname,agent-hostdomainname,agent-version,agent-id,agent-
connector-name,agent-group,event-source-hostname,event-source-
hostdomainname,event-source-address,event-source-processname,receiver-
name,receiver-hostname,receiver-hostaddress,receiver-hostdomainname,receiver-
port,receiver-time-gmt,receiver-timezone,receiver-version,event-protocol,event-
logname,event-euuid,event-count,event-summarized,event-duration,event-time-
year,event-time-month,event-time-monthday,event-time-weekday,event-time-
hour,event-time-minute,event-time-gmt,event-datetime,event-year-datetime,event-
month-datetime,event-day-datetime,event-hour-datetime,event-quarterhour-
datetime,event-minute-datetime,event-timezone,event-sequence,event-trend,event-
action,event-id,event-category,event-class,ideal-model,event-severity,event-
result,result-string,result-signature,result-code,result-version,result-
priority,result-scope,result-severity,raw-event,snippet }
    STATUS  current
    DESCRIPTION
            "The ELM SNMP Trap."
    ::= { elmAlertTrapGroup 1 }
```

L'elmAlertTrapGroup è 1.3.6.1.4.1.791.9845.3 e l'elmtrap è definita dal nodo successivo. Per impostazione predefinita, l'ID di elmTrap è 1.3.6.1.4.1.791.9845.3.1. L'intervallo degli ID di trap personalizzati definiti dall'utente è compreso tra 1.3.6.1.4.1.791.9845.3.2 e 1.3.6.1.4.1.791.9845.3.999.

Importante: Per l'invio di trap a CA Spectrum, si consiglia l'utilizzo dell'ID predefinito di elmTrap. Per l'invio di trap a CA NSM, si consiglia di specificare un ID di trap personalizzato collegato ad un ID elmTrap in una MIB personalizzata.

Mapping da OID (ID oggetto) a campo di CEG

Nella seguente tabella sono visualizzati i campi CEG corrispondenti ad ogni ID oggetto (OID) in elmAlertVariables nell'albero della MIB. Questo ramo dell'albero si estenderà man mano che verranno aggiunti nuovi campi alla CEG. Controllare gli aggiornamenti della MIB e verificare la disponibilità dell'ultima versione per i prodotti di destinazione dei trap SNMP.

ID oggetto (OID)	Campo CEG
1.3.6.1.4.1.791.9845.2.1	source-username
1.3.6.1.4.1.791.9845.2.2	source-domainname
1.3.6.1.4.1.791.9845.2.3	source-groupname
1.3.6.1.4.1.791.9845.2.4	source-uid
1.3.6.1.4.1.791.9845.2.5	source-gid
1.3.6.1.4.1.791.9845.2.6	source-hostname
1.3.6.1.4.1.791.9845.2.7	source-hostdomainname
1.3.6.1.4.1.791.9845.2.8	source-address
1.3.6.1.4.1.791.9845.2.9	source-mac-address
1.3.6.1.4.1.791.9845.2.10	source-port
1.3.6.1.4.1.791.9845.2.11	source-processname
1.3.6.1.4.1.791.9845.2.12	source-objectname
1.3.6.1.4.1.791.9845.2.13	source-objectattr
1.3.6.1.4.1.791.9845.2.14	source-objectid
1.3.6.1.4.1.791.9845.2.15	source-objectclass
1.3.6.1.4.1.791.9845.2.16	source-objectvalue
1.3.6.1.4.1.791.9845.2.17	dest-username
1.3.6.1.4.1.791.9845.2.18	dest-domainname
1.3.6.1.4.1.791.9845.2.19	dest-groupname
1.3.6.1.4.1.791.9845.2.20	dest-uid
1.3.6.1.4.1.791.9845.2.21	dest-gid
1.3.6.1.4.1.791.9845.2.22	dest-hostname
1.3.6.1.4.1.791.9845.2.23	dest-hostdomainname

ID oggetto (OID)	Campo CEG
1.3.6.1.4.1.791.9845.2.24	dest-address
1.3.6.1.4.1.791.9845.2.25	dest-mac-address
1.3.6.1.4.1.791.9845.2.26	dest-port
1.3.6.1.4.1.791.9845.2.27	dest-objectname
1.3.6.1.4.1.791.9845.2.28	dest-objectattr
1.3.6.1.4.1.791.9845.2.29	dest-objectid
1.3.6.1.4.1.791.9845.2.30	dest-objectclass
1.3.6.1.4.1.791.9845.2.31	dest-objectvalue
1.3.6.1.4.1.791.9845.2.32	agent-name
1.3.6.1.4.1.791.9845.2.33	agent-address
1.3.6.1.4.1.791.9845.2.34	agent-hostname
1.3.6.1.4.1.791.9845.2.35	agent-hostdomainname
1.3.6.1.4.1.791.9845.2.36	agent-version
1.3.6.1.4.1.791.9845.2.37	agent-id
1.3.6.1.4.1.791.9845.2.38	agent-connector-name
1.3.6.1.4.1.791.9845.2.39	agent-group
1.3.6.1.4.1.791.9845.2.40	event-source-hostname
1.3.6.1.4.1.791.9845.2.41	event-source-hostdomainname
1.3.6.1.4.1.791.9845.2.42	event-source-address
1.3.6.1.4.1.791.9845.2.43	event-source-processname
1.3.6.1.4.1.791.9845.2.44	receiver-name
1.3.6.1.4.1.791.9845.2.45	receiver-hostname
1.3.6.1.4.1.791.9845.2.46	receiver-hostaddress
1.3.6.1.4.1.791.9845.2.47	receiver-hostdomainname
1.3.6.1.4.1.791.9845.2.48	receiver-port
1.3.6.1.4.1.791.9845.2.49	receiver-time-gmt
1.3.6.1.4.1.791.9845.2.50	receiver-timezone
1.3.6.1.4.1.791.9845.2.51	receiver-version

ID oggetto (OID)	Campo CEG
1.3.6.1.4.1.791.9845.2.52	event-protocol
1.3.6.1.4.1.791.9845.2.53	event-logname
1.3.6.1.4.1.791.9845.2.54	event-euuid
1.3.6.1.4.1.791.9845.2.55	event-count
1.3.6.1.4.1.791.9845.2.56	event-summarized
1.3.6.1.4.1.791.9845.2.57	event-duration
1.3.6.1.4.1.791.9845.2.58	event-time-year
1.3.6.1.4.1.791.9845.2.59	event-time-month
1.3.6.1.4.1.791.9845.2.60	event-time-monthday
1.3.6.1.4.1.791.9845.2.61	event-time-weekday
1.3.6.1.4.1.791.9845.2.62	event-time-hour
1.3.6.1.4.1.791.9845.2.63	event-time-minute
1.3.6.1.4.1.791.9845.2.64	event-time-gmt
1.3.6.1.4.1.791.9845.2.65	event-datetime
1.3.6.1.4.1.791.9845.2.66	event-year-datetime
1.3.6.1.4.1.791.9845.2.67	event-month-datetime
1.3.6.1.4.1.791.9845.2.68	event-day-datetime
1.3.6.1.4.1.791.9845.2.69	event-hour-datetime
1.3.6.1.4.1.791.9845.2.70	event-quarterhour-datetime
1.3.6.1.4.1.791.9845.2.71	event-minute-datetime
1.3.6.1.4.1.791.9845.2.72	event-timezone
1.3.6.1.4.1.791.9845.2.73	event-sequence
1.3.6.1.4.1.791.9845.2.74	event-trend
1.3.6.1.4.1.791.9845.2.75	event-action
1.3.6.1.4.1.791.9845.2.76	event-id
1.3.6.1.4.1.791.9845.2.77	event-category
1.3.6.1.4.1.791.9845.2.78	event-class
1.3.6.1.4.1.791.9845.2.79	ideal-model

ID oggetto (OID)	Campo CEG
1.3.6.1.4.1.791.9845.2.80	event-severity
1.3.6.1.4.1.791.9845.2.81	event-result
1.3.6.1.4.1.791.9845.2.82	result-string
1.3.6.1.4.1.791.9845.2.83	result-signature
1.3.6.1.4.1.791.9845.2.84	result-code
1.3.6.1.4.1.791.9845.2.85	result-version
1.3.6.1.4.1.791.9845.2.86	result-priority
1.3.6.1.4.1.791.9845.2.87	result-scope
1.3.6.1.4.1.791.9845.2.88	result-severity
1.3.6.1.4.1.791.9845.2.89	raw-event

MIB personalizzate

È possibile creare file MIB personalizzati a partire dal testo standard fornito ed aggiungendo le varbind selezionate dal contenuto del file CA-ELM.MIB. Un file MIB personalizzato per un singolo avviso contiene un sottoinsieme dei contenuti del file CA-ELM.MIB file. Le differenze tra un file MIB personalizzato per un avviso ed il file CA-ELM.MIB sono le seguenti:

- Il file MIB personalizzato consente di definire soltanto i campi inviati dall'avviso.
- Il file MIB personalizzato consente di definire una trap contenente suddetti campi in base all'ordine di invio.
- La trap MIB personalizzata viene definita con l'OID 1.3.6.1.4.1.791.9845.3.x, dove x corrisponde a un valore compreso tra 1 e 999.

  Nota: un avviso che utilizza una MIB personalizzata specifica l'OID come valore per l'ID di trap personalizzata.
- Una MIB personalizzata include la varbind dynamicData *solo se* la query contiene i campi calcolati.

  I calcoli possono essere applicati a qualsiasi campo. Il campo event_count costituisce un esempio di campo a cui vengono solitamente applicati i calcoli. Esistono, tuttavia, delle eccezioni. Nella query System Event Count by Event Action (Conteggio degli eventi di sistema per Azione evento), il campo Event_count viene calcolato con Sum. Per determinare se un campo viene calcolato, esaminare la query di definizione del campo. Di seguito viene riportato un esempio di definizione di event_count come campo calcolato:

  ```
  System_Event_Count_By_Event_Action.xml:    <Column columnname="event_count"
  datatype="I" displayname="Count" functionname="sum" resultname="event_count"
  sortdesc="true" sortorder="1" visible="true"/>
  ```

Testo standard per una MIB personalizzata

Di seguito viene riportato il testo standard per una MIB personalizzata. Se si avvia una MIB personalizzata con questo esempio, è possibile sostituire o inserire dati personalizzati nelle posizioni indicate dalla stringa ###. Nelle sezioni in cui si modificano i dati è inoltre possibile modificare la descrizione.

```
CAELM-MIB DEFINITIONS ::= BEGIN
  IMPORTS
        MODULE-IDENTITY, OBJECT-TYPE, Integer32, NOTIFICATION-TYPE
                 FROM SNMPv2-SMI
MODULE-COMPLIANCE, OBJECT-GROUP,NOTIFICATION-GROUP
                 FROM SNMPv2-CONF                        DisplayString
                FROM SNMPv2-TC
```

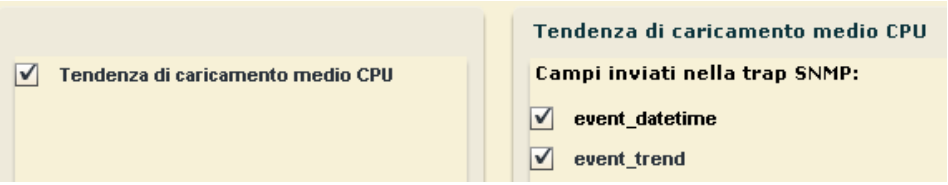
```
elm MODULE-IDENTITY
    LAST-UPDATED "200907050600Z"
    ORGANIZATION "CA"
    CONTACT-INFO
        "100 Staples drive
        Framingham MA"
    DESCRIPTION
        "Contains objects describing data for ELM events"
    REVISION "200907050600Z"
    DESCRIPTION
        "Custom MIB <###>."
    ::= { ca 9845 }

ca OBJECT IDENTIFIER ::= {enterprises 791}
elmAlertTrapGroup OBJECT IDENTIFIER ::= { elm 3 }
elmAlertVariables OBJECT IDENTIFIER ::= { elm 2 }
elmDynamicVariables OBJECT IDENTIFIER ::= { elm 4 }
elmConformance OBJECT IDENTIFIER ::= { elm 5 }
elmGroups      OBJECT IDENTIFIER ::= { elmConformance 1 }
elmCompliances OBJECT IDENTIFIER ::= { elmConformance 2 }


<### Inserire la varbind elmAlertVariable per ogni campo di query ###>

<### Inserire la seguente varbind di dynamicData solo se le query includono campi
calcolati ###>
dynamicData OBJECT-TYPE
    SYNTAX  DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
" This field contains all the elm dynamic variables and data in name=value
format."
    ::= { elmDynamicVariables 2 }

calmAPIURL OBJECT-TYPE
    SYNTAX  OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
"The OPEN API URL which points to the query result."
    ::= { elmDynamicVariables 1 }
```

```
elmTrap NOTIFICATION-TYPE
    OBJECTS { <### Inserire l'elenco dei campi di query con trattini ###> }
    STATUS  current
    DESCRIPTION
            "The ELM SNMP Trap."
    ::= { elmAlertTrapGroup <### inserire il numero del nodo dell'ID di trap
personalizzato ###> }

elmCompliance MODULE-COMPLIANCE
    STATUS  current
    DESCRIPTION
            "The compliance information."
    MODULE  -- this module
        GROUP       elmDataGroup
        DESCRIPTION
            "This group is mandatory."
    ::= { elmCompliances 3 }
-- units of conformance

elmDataGroup    OBJECT-GROUP
    OBJECTS { <### Inserire l'elenco dei campi di query con trattini ###> }
    STATUS  current
    DESCRIPTION
            "A collection of objects providing information specific to
            ELM data."
    ::= { elmGroups 1 }
END
```

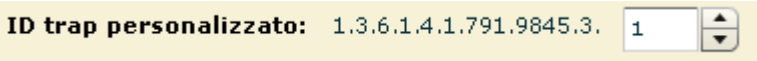
Esempio: Creazione di una MIB 33 personalizzata per la query della tendenza di caricamento medio CPU

Creare una MIB personalizzata per ogni query inviata a CA NSM come trap SNMP. Ogni query è associata ad un ID di trap personalizzato. La MIB personalizzata definisce i campi selezionati da includere nella trap nell'ordine visualizzato nell'avviso.

Considerare l'esempio in cui la query selezionata per l'avviso corrisponde alla tendenza di caricamento medio CPU. I campi selezionati sono event_datetime e event_trend.



L'ID di trap personalizzato corrisponde a 1.3.6.1.4.1.791.9845.3.33.



Per creare una MIB personalizzata per l'ID di trap personalizzato terminante in 33

1. Aprire una copia di CA-ELM.MIB per copiare il testo nella propria MIB personalizzata.
2. Aprire un editor, copiare il testo standard per la MIB personalizzata e salvare il file con un nuovo nome. Ad esempio, salvare il file come Custom MIB n.mib, dove n corrisponde a 33, ovvero il nodo finale dell'ID di trap personalizzato specificato per la query dell'avviso.
3. (Facoltativo) in elm MODULE-IDENTITY, sostituire <###> con 33. Ad esempio:

   ```
   MIB 33 personalizzata."
   ```

4. Sostituire il seguente testo standard con il testo di CA-ELM.MIB

   ```
   <### Inserire la varbind elmAlertVariable per ogni campo di query nella
   sequenza di trap ###>
   ```

   Copiare le varbind elmAlertVariable per event_datetime e per event_trend. Queste varbind devono essere visualizzate nella MIB nella stessa sequenza di invio alla trap SNMP. Ad esempio:

   ```
   event-datetime OBJECT-TYPE
       SYNTAX  DisplayString
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIZIONE
   "Data e Ora espresse nelle informazioni evento"
       ::= { elmAlertVariables 65 }

   event-trend OBJECT-TYPE
       SYNTAX  Integer32
       MAX-ACCESS  read-only
       STATUS      current
       DESCRIZIONE
   "Trending data for this event."
       ::= { elmAlertVariables 74 }
   ```

5. Nessuno dei campi in questa query è un campo calcolato. Eliminare il seguente testo standard:

```
<### Inserire la seguente varbind di dynamicData solo se le query includono
campi calcolati ###>
dynamicData OBJECT-TYPE
    SYNTAX  DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIZIONE
" This field contains all the elm dynamic variables and data in name=value
format."
    ::= { elmDynamicVariables 2 }
```

6. Sostituire il seguente testo standard in elmTrap:

```
OBJECTS { <### Inserire l'elenco dei campi di query con trattini ###> }
```

con l'elenco dei campi di query selezionati, come indicato di seguito:

```
OBJECTS { event-datetime,event-trend }
```

7. Sostituire il seguente testo standard in elmTrap:

```
::= { elmAlertTrapGroup <### inserire il numero del nodo dell'ID di trap
personalizzato ###> }
```

con il seguente:

```
::= { elmAlertTrapGroup 33 }
```

8. Sostituire il seguente testo standard in elmDataGroup:

```
OBJECTS { <### Inserire l'elenco dei campi di query con trattini ###> }
```

con il seguente:

```
OBJECTS { event-datetime,event-trend }
```

9. Salvare il file.

Esempio: MIB 33 personalizzata

L'esempio seguente è una MIB personalizzata sviluppata per un avviso inviato come trap SNMP con l'ID di trap personalizzato terminante in 33. L'ID di trap personalizzato corrispondeva a 1.3.6.1.4.1.791.9845.3.33. La query selezionata corrispondeva a Tendenza di caricamento medio CPU ed i campi selezionati da inviare nella trap SNMP sono event_datetime ed event_trend.

```
CAELM-MIB DEFINITIONS ::= BEGIN
  IMPORTS
        MODULE-IDENTITY, OBJECT-TYPE, Integer32, NOTIFICATION-TYPE
                FROM SNMPv2-SMI
MODULE-COMPLIANCE, OBJECT-GROUP,NOTIFICATION-GROUP
                FROM SNMPv2-CONF                        DisplayString
               FROM SNMPv2-TC

elm MODULE-IDENTITY
    LAST-UPDATED "200907050600Z"
    ORGANIZATION "CA"
    CONTACT-INFO
        "100 Staples drive
        Framingham MA"
    DESCRIPTION
        "Contains objects describing data for ELM events"
    REVISION "200907050600Z"
    DESCRIPTION
        "Custom MIB 33."
    ::= { ca 9845 }

ca OBJECT IDENTIFIER ::= { enterprises 791}
elmAlertTrapGroup OBJECT IDENTIFIER ::= { elm 3 }
elmAlertVariables OBJECT IDENTIFIER ::= { elm 2 }
elmDynamicVariables OBJECT IDENTIFIER ::= { elm 4 }
elmConformance OBJECT IDENTIFIER ::= { elm 5 }
elmGroups      OBJECT IDENTIFIER ::= { elmConformance 1 }
elmCompliances OBJECT IDENTIFIER ::= { elmConformance 2 }

event-datetime OBJECT-TYPE
    SYNTAX  DisplayString
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
"The calendar date and time expressed in the event information"
    ::= { elmAlertVariables 65 }
```

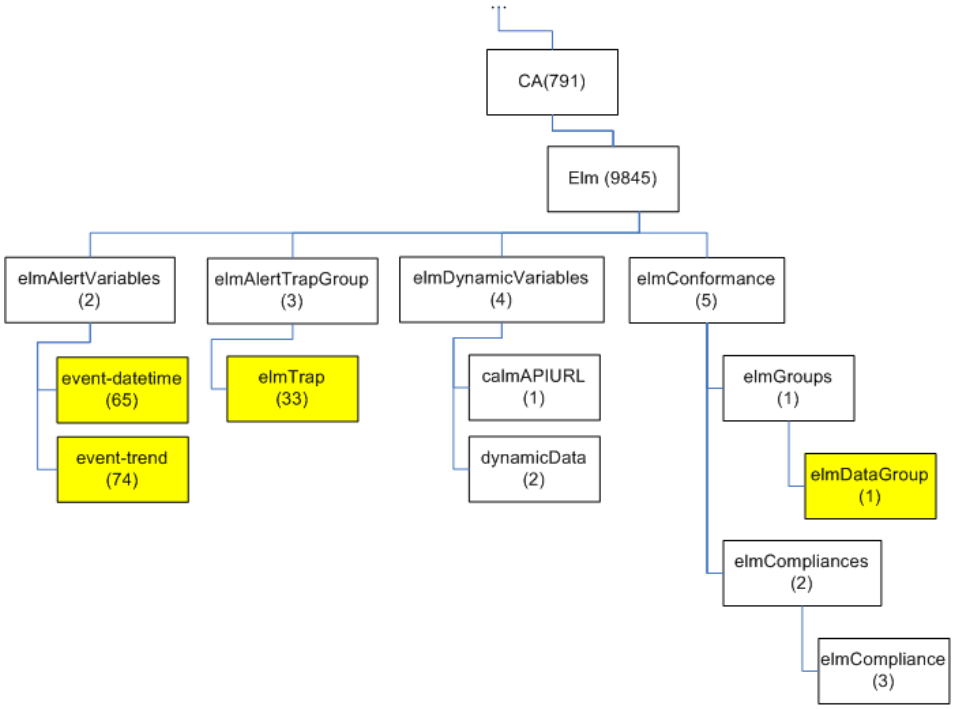
```
event-trend OBJECT-TYPE
    SYNTAX  Integer32
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
"Trending data for this event."
    ::= { elmAlertVariables 74 }

calmAPIURL OBJECT-TYPE
    SYNTAX  OCTET STRING
    MAX-ACCESS  read-only
    STATUS      current
    DESCRIPTION
"The OPEN API URL which points to the query result."
    ::= { elmDynamicVariables 1 }

elmTrap NOTIFICATION-TYPE
    OBJECTS { event-datetime,event-trend }
    STATUS  current
    DESCRIPTION
            "The ELM SNMP Trap."
    ::= { elmAlertTrapGroup 33 }

elmCompliance MODULE-COMPLIANCE
    STATUS  current
    DESCRIPTION
            "The compliance information."
    MODULE  -- this module
        GROUP       elmDataGroup
        DESCRIPTION
            "This group is mandatory."
    ::= { elmCompliances 3 }
-- units of conformance

elmDataGroup    OBJECT-GROUP
    OBJECTS {  event-datetime,event-trend }
    STATUS  current
    DESCRIPTION
            "A collection of objects providing information specific to
            ELM data."
    ::= { elmGroups 1 }
END
```

Esempio: Struttura MIB per MIB 33 personalizzate

Le differenze tra la struttura MIB per una MIB personalizzata e quella per CA-ELM.MIB sono le seguenti:

- Gli oggetti di elmAlertVariables in elmalertVariables sono limitati ai campi della query. Considerare il seguente esempio, in cui i campi selezionati sono:
  - event_datetime
  - event_trend
- L'elmTrap contenente solo i campi di query sostituisce elmTrap (1) in CA-ELM.MIB, il quale contiene tutti i campi CEG. Considerare l'esempio in cui l'elmTrap è 33. Questo identificatore di elmTrap fa riferimento al nodo finale dell'ID di trap personalizzato, 1.3.6.1.4.1.791.9845.3.33.

Di seguito viene riportata una descrizione della MIB 33personalizzata nel formato di struttura MIB. I blocchi evidenziati indicano le differenze tra la MIB personalizzata e CA-ELM.MIB. La MIB personalizzata definisce soltanto due campi di elmAlertVariables. L'elmTrap personalizzato comprende soltanto due campi di query ed ha un numero univoco: 33. L'elmDataGroup comprende soltanto due campi di query.



Considerazioni sull'utilizzo di MIB

Per fare in modo che un sistema comprenda le trap SNMP ricevute da CA User Activity Reporting Module mediante MIB, il sistema dovrà conoscere quanto definito dagli identificatori dell'oggetto (OID, Object Identifier) in composizione. Di seguito vengono riportati i requisiti:

- Importare il file CA-ELM.MIB, compilarlo e mantenerlo aggiornato.
- (Solo CA NSM) Creare, importare e compilare una MIB personalizzata per ciascun avviso pianificato inviato come trap SNMP.

  Nota: è possibile utilizzare la stessa MIB personalizzata per avvisi basati su query che inviano gli stessi campi nello stesso ordine di una trap.

  Ad esempio, le seguenti query restituiscono tutti i valori per i campi dest_hostname ed event_count.

  - Cinque accessi al sistema non riusciti per Sistema
  - Riepilogo attività di ripristino non riuscite negli ultimi sette giorni per Host
  - Riepilogo attività di backup non riuscite negli ultimi sette giorni per Host
  - Numero eccessivo di errori di configurazione (25) registrate nell'ultima ora
  - Numero eccessivo di modifiche di configurazione (25) registrate nell'ultima ora
  - Numero eccessivo di attività SU (25) registrate nell'ultima ora
  - Aggregazione eventi critici o irrecuperabili su host critico

  Se si creano avvisi separati basati su queste query, tali avvisi specificheranno lo stesso ID di trap personalizzata e verranno interpretati con la stessa MIB personalizzata.

Gli utenti che controllano le trap SNMP ricevute nel prodotto di destinazione possono interpretare le trap inviate da CA User Activity Reporting Module in due modi differenti:

- Avviando la pagina dei risultati delle trap SNMP mediante l'URL inviato nella trap.
- Utilizzando un'applicazione che fa riferimento alle MIB importate.

Processo di utilizzo dei trap SNMP

L'utilizzo delle trap SNMP prevede le seguenti procedure:

1. Preparare CA User Activity Reporting Module per l'invio di trap SNMP.
   - Configurare la destinazione di trap SNMP predefinita.
   - Identificare l'indirizzo IP e la porta di ogni destinazione di trap SNMP aggiuntiva che è possibile specificare al momento dell'invio degli avvisi come trap SNMP.
   - Identificare gli avvisi i cui risultati di query possono essere di interesse per CA Spectrum, per CA NSM o per un altro ricevitore delle trap SNMP.
2. Preparare i prodotti di destinazione di trap SNMP per la ricezione delle trap SNMP di CA User Activity Reporting Module
   - Se CA Spectrum dovrà essere una destinazione:
     - Creare un modello di evento attenendosi alla documentazione di Spectrum. Senza un modello di evento, non è possibile visualizzare i risultati di trap nella destinazione.
     - Configurare CA Spectrum per la ricezione di trap SNMP v3.
   - Se CA NSM dovrà essere una destinazione:
     - Installare la build di NSM r11.2 GA su Windows Server 2003 EE SP1 ed applicare la patch per aggiornare il file aws_snmpex.dll.
     - Configurare CA NSM per la ricezione delle trap SNMP, comprese le trap SNMP v3.

3. (Facoltativo) preparare la destinazione di trap SNMP per interpretare le trap SNMP provenienti da CA User Activity Reporting Module mediante i file MIB.
   - Scaricare la MIB di CA User Activity Reporting Module in un percorso accessibile dal prodotto di destinazione di trap SNMP.

     Nota: il file CA-ELM.MIB è presente nel DVD di installazione. È possibile scaricare l'ultima versione di questa MIB dalla pagina di prodotto di CA User Activity Reporting Module.
   - Importare e compilare il file CA-ELM.MIB.
   - (Solo CA NSM) per ogni avviso da inviare come trap SNMP, creare una MIB personalizzata mediante una trap definita con 1.3.6.1.4.1.791.9845.3.x, dove x corrisponde ad un numero intero uguale a o minore di 999. Importare e compilare tutte le MIB personalizzate.

   Importante: Si tratta di un passaggio facoltativo, in quanto le trap ricevute da CA User Activity Reporting Module possono essere interpretate mediante l'avvio della pagina dei risultati delle trap a partire dall'URL inviato nella trap.
4. Pianificare gli avvisi con le destinazioni di trap SNMP.
5. Verificare che l'avviso sia stato inviato come una trap SNMP.
6. (Facoltativo) Controllare i risultati delle trap SNMP inviate a partire dalla destinazione di trap.
   - Visualizzare i risultati della trap SNMP nella destinazione di trap.
   - Aprire l'URL per visualizzare i dati inviati dall'avviso in formato di diagramma o di grafico.

Configurare l'integrazione con una destinazione di trap SNMP

Configurare l'integrazione SNMP come parte della configurazione globale di servizio per il server di rapporto. La configurazione corrisponde all'indirizzo IP e alla porta della destinazione dei trap SNMP.

È possibile configurare l'integrazione SNMP sia prima che dopo aver preparato il prodotto di destinazione a ricevere e ad interpretare i trap SNMP di CA User Activity Reporting Module.

Quando si crea un avviso indirizzato al destinatario di un trap SNMP, è possibile specificare una o più destinazioni. Questa configurazione sarà quella predefinita. L'impostazione predefinita verrà applicata a tutti server elencati in Server di rapporto.

Per configurare l'integrazione SNMP

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
2. Fare clic su Servizio di avviso.
3. Immettere l'indirizzo IP o il nome host del server di destinazione per le trap SNMP.
4. Accettare la porta predefinita, 162, oppure modificarla.
5. Fare clic su Salva.

Preparare CA Spectrum per ricevere le trap SNMP dagli avvisi

È possibile inviare gli avvisi sottoforma di trap SNMP da CA User Activity Reporting Module a qualsiasi destinazione della rete in grado di ricevere ed interpretare le trap. Ogni prodotto che riceve trap possiede i propri requisiti.

Preparare CA Spectrum per la ricezione di trap dagli avvisi di CA User Activity Reporting Module mediante:

- Integrazione di CA Spectrum Southbound Gateway, un punto d'integrazione in grado di supportare qualsiasi formato di flusso dati di avviso proveniente da un sistema di terze parti, compresi i trap SNMP come quelli generati da CA User Activity Reporting Module.
- Creazione di un modello del nodo CA User Activity Reporting Module per abilitare la ricezione delle trap SNMP v3.
- Download del MIB di CA User Activity Reporting Module.
- Importazione del MIB di CA User Activity Reporting Module in CA Spectrum.

il processo di integrazione di Southbound Gateway è interamente documentato nella *Guida al toolkit di Spectrum Southbound Gateway*. L'integrazione di Southbound Gateway include il mapping delle trap SNMP agli eventi CA Spectrum in un file AlertMap e la definizione dei modelli richiesti. Il punto di integrazione di Southbound Gateway accetta i dati di avviso da sistemi di terze parti e consente di visualizzarli in OneClick.

Una volta scaricato il file MIB dalla pagina di prodotto di CA User Activity Reporting Module sul sito del supporto tecnico o dopo averlo ottenuto dai DVD di installazione, sarà possibile importarlo in CA Spectrum. Per ulteriori informazioni sull'utilizzo dello strumento MIB per l'importazione in CA Spectrum OneClick, consultare la *Guida alla gestione di dispositivi CA Spectrum*.

Configurare CA Spectrum per ricevere trap SNMP v3

Per inviare trap SNMP v3 da CA User Activity Reporting Module a CA Spectrum, occorre creare un modello del dispositivo di CA User Activity Reporting Module in CA Spectrum. I trap SNMP v3 verranno quindi indirizzati al nodo di CA User Activity Reporting Module modellato dall'utente.

Per creare un modello che consenta a Spectrum di ricevere trap SNMP v3 dagli avvisi

1. Accedere al server Windows su cui è installato CA Spectrum.
2. Accedere alla console di Spectrum OneClick:
   a. Fare clic su Start, Tutti i programmi, CA, Pannello di controllo di SPECTRUM.

      Il pannello di controllo di SPECTRUM viene visualizzato con un indicatore di Stato nella parte inferiore dello schermo.

   b. Se Stato non visualizza RUNNING (in esecuzione), fare clic su Avvia SpectroSERVER in Controllo di processo.

   c. Quando Stato visualizza RUNNING (in esecuzione), fare clic su Amministrazione di OneClick.

      Amministrazione di OneClick - il pannello di controllo di SPECTRUM viene visualizzato con Host su localhost e Porta su 80.

   d. Fare clic su OK

      Viene visualizzata una finestra di dialogo di accesso.

   e. Inserire le credenziali.

      Viene visualizzata la pagina di Spectrum NFM OneClick.

   f. Fare clic su Avvia console.

      Viene visualizzata la finestra di accesso "Accesso - SPECTRUM OneClick", che consente di collegarsi a SPECTRUM OneClick sull'host locale.

   g. Fare clic su OK

      Viene visualizzata la finestra Console - SPECTRUM OneClick con i riquadri Navigazione, Contenuto e Dettagli componente.

3. Nella scheda Explorer del riquadro Navigazione, espandere il nodo di livello superiore e selezionare Universe.

   I titoli dei riquadri Contenuto e Dettagli componente visualizzano Universe di tipo Universe.

4. Nel riquadro Contenuto, fare clic sulla scheda Topologia.

   Il secondo pulsante della scheda consente di creare un nuovo modello in base al tipo e di aggiungerlo a questa visualizzazione.

5. Fare clic su Crea nuovo modello.

   Viene visualizzata la finestra di dialogo "Seleziona tipo di modello - SPECTRUM OneClick".

6. Fare clic sulla scheda Tutti i tipi di modello.

7. Digitare una stringa nel campo Filtro. Ad esempio, digitare gn.

   Nell'elenco verranno visualizzati i tipi di modello che iniziano con Gn.

8. Selezionare il tipo di modello desiderato e fare clic su OK. Ad esempio, selezionare GnSNMPDev e fare clic su OK.

   Viene visualizzata la finestra Crea modello di tipo <selected model type>.

9. Completare la finestra di dialogo Crea modello di tipo attenendosi a quanto riportato di seguito:

   a. Nel campo Nome, immettere il nome di host del server CA User Activity Reporting Module.

   b. Nel campo Indirizzo di rete, inserire l'indirizzo IP dello stesso server.

   c. Se l'impostazione predefinita 161 non è quella desiderata, inserire il numero di porta nel campo Porta agente. Ad esempio, immettere 162.

   d. Selezionare SNMP v3 come opzione di Comunicazione SNMP.

   e. Fare clic su Profili.

   Viene visualizzata la finestra Modifica profili SNMP v3, insieme ad un elenco degli eventuali profili esistenti.

10. Per aggiungere un profilo, attenersi alla procedura riportata di seguito:
    a. Digitare il nome di profilo e l'ID utente.
    b. Poichè ciò vale per gli SNMP v3, come tipo di autenticazione selezionare Autenticazione con riservatezza.
    c. Nei quattro campi successivi, digitare due volte una password di autenticazione di 8 caratteri e una di riservatezza, sempre di 8 caratteri.
    d. Fare clic su Aggiungi per aggiungere il profilo all'elenco.
    e. Fare clic su OK.

    Il profilo aggiunto viene visualizzato prima nell'elenco a discesa Profilo v3 della finestra di dialogo Crea modello di tipo.
11. Selezionare Rileva connessioni e fare clic su OK.

    Viene visualizzato l'indicatore di avanzamento Creazione del modello. Una volta completata l'elaborazione, il modello creato viene visualizzato sotto forma di grafico nella scheda Topologia, con il nome di host inserito e il tipo di modello selezionato.

Download del MIB di CA User Activity Reporting Module

È possibile scaricare il file MIB (Management Information Base) dalla pagina di prodotto di CA User Activity Reporting Module sul sito del supporto tecnico, oppure prelevarlo dal DVD di installazione. Una volta scaricato il MIB di CA User Activity Reporting Module, è possibile importarlo e compilarlo in ogni prodotto configurato come destinazione di trap SNMP.

Per scaricare il MIB di CA User Activity Reporting Module

1. Accedere al server in cui è installato CA Spectrum
2. Avviare CA Support Online ed eseguire l'accesso.
3. Accedere alla pagina di prodotto di CA User Activity Reporting Module.
4. Scaricare il file MIB di CA User Activity Reporting Module in rete.
5. Se si prevede di inviare trap SNMP a CA Spectrum, importare il MIB di CA User Activity Reporting Module in CA Spectrum.
6. Se si prevede di inviare trap SNMP a CA NSM, importare il MIB di CA User Activity Reporting Module in CA NSM. Per la procedura, fare riferimento alla documentazione di CA NSM.

Importare il CAELM-MIB in CA Spectrum

Prima di inviare trap SNMP da CA User Activity Reporting Module a CA Spectrum, è possibile importare e compilare il MIB di CA User Activity Reporting Module utilizzando gli strumenti MIB OneClick di CA Spectrum.

Nota: i MIB SNMPv2 a cui viene fatto riferimento in CA-ELM.MIB sono precaricati in CA Spectrum.

Per importare CA-ELM.MIB in CA Spectrum

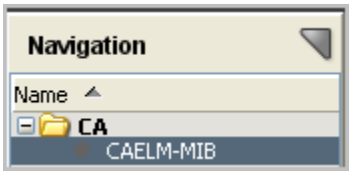
1. Accedere a CA Spectrum.
2. Avviare la console OneClick.
3. Fare clic su Strumenti, Utilità, Strumenti MIB.

   Verrà visualizzata la finestra di dialogo Strumenti MIB: Aggiungi MIB.
4. Fare clic su Sfoglia, raggiungere il percorso in cui è stato scaricato il file CA-ELM.MIB e selezionare il file.
5. Fare clic su Compila.

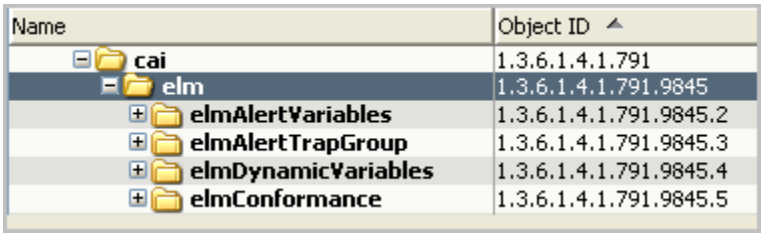
   Un messaggio di conferma indicherà che il MIB di CA User Activity Reporting Module è stato memorizzato nella seguente directory del server Web di OneClick:

   `<$SPECROOT>/MibDatabase/userContrib`
6. Chiudere la finestra di dialogo Strumenti MIB: Aggiungi MIB.

   CAELM-MIB verrà aggiunto alla barra di Navigazione, in CA.



   Nella gerarchia, cai si espanderà in modo da visualizzare elm con i relativi oggetti subordinati della struttura e gli OID associati.



Name	Object ID
cai	1.3.6.1.4.1.791
elm	1.3.6.1.4.1.791.9845
elmAlertVariables	1.3.6.1.4.1.791.9845.2
elmAlertTrapGroup	1.3.6.1.4.1.791.9845.3
elmDynamicVariables	1.3.6.1.4.1.791.9845.4
elmConformance	1.3.6.1.4.1.791.9845.5

Esempio: avvisare CA Spectrum delle modifiche alla configurazione

Prima di inviare trap SNMP a CA Spectrum per la prima volta, è opportuno identificare le query che restituiscono risultati pertinenti con tale destinazione. Quando si pianifica il primo avviso con Spectrum come destinazione, è possibile seguire l'avanzamento e confrontare i risultati visualizzati in CA User Activity Reporting Module con quelli visualizzati nell'interfaccia di CA Spectrum. Una volta che l'invio di trap a CA Spectrum sarà un'operazione di routine, sarà possibile ignorare i passaggi di preparazione e follow-up.

L'esempio seguente fornisce le indicazioni per eseguire il processo iniziale, fra cui:

- Preparare l'invio dei trap SNMP a CA Spectrum
- Inviare trap SNMP a CA Spectrum
- Verificare l'effettivo invio dei trap SNMP
- Visualizzare i trap SNMP ricevuti da CA Spectrum

Ulteriori informazioni:

Inviare trap SNMPv2 a CA Spectrum (a pagina 451)
Seguire l'avanzamento dei processi di avviso (a pagina 454)
Visualizzare trap SNMP in CA Spectrum (a pagina 455)

Inviare trap SNMPv2 a CA Spectrum

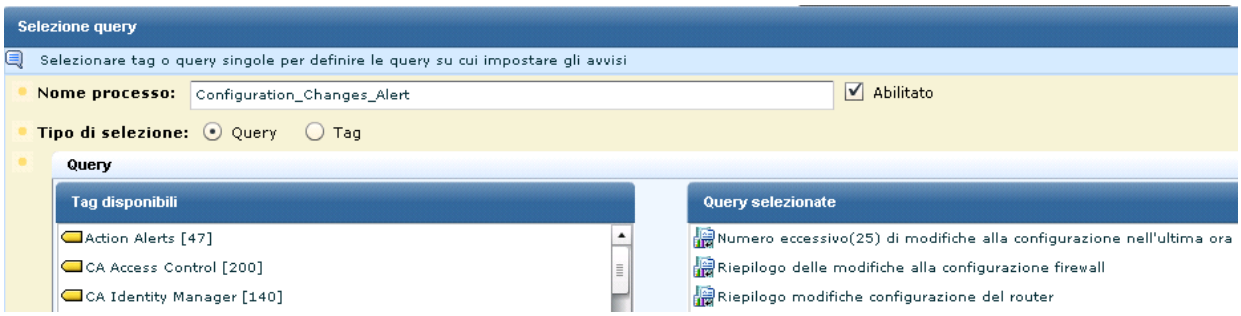
Il seguente esempio illustra come creare un avviso che notifica CA Spectrum delle modifiche di configurazione utilizzando trap SNMP v2.

Per preparare l'invio dei trap SNMPv2 a CA Spectrum

1. Aprire la procedura guidata Pianificazione avviso.
   a. Fare clic sulla scheda Gestione avvisi e quindi sulla sottoscheda Pianificazione avvisi.
   b. Fare clic sul pulsante Pianifica un avviso.

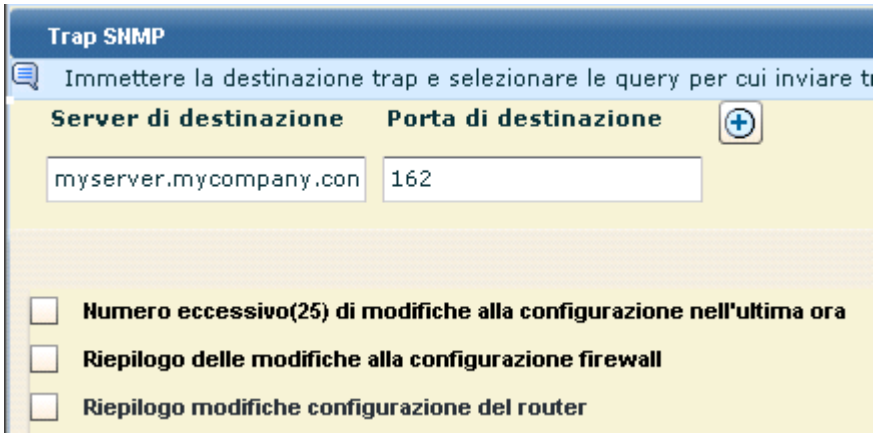
2. Eseguire il passaggio Selezione avviso.
   a. Digitare il nome di processo. Questa operazione è necessaria per qualsiasi avviso.
   b. Verificare che il tipo di selezione sia Query.

      Non è consentito selezionare le destinazioni di trap SNMP per gli avvisi basati sui tag.
   c. Se le query da selezionare sono contrassegnate come Avvisi, fare clic sul tag Avvisi per filtrare l'elenco visualizzato.
   d. Selezionare la query o le query identificate.



3. (Facoltativo) Eseguire i passaggi Filtri di avviso, Condizioni di risultato e Pianifica processi, come documentato nella Guida in linea per questa procedura guidata.
4. Impostare i dettagli sui trap SNMP.
   a. Fare clic sul passaggio Destinazione.
   b. Selezionare la scheda Trap SNMP.

      Verranno visualizzate la destinazione dei trap SNMP configurata e le query selezionate al passaggio 1 della procedura guidata.

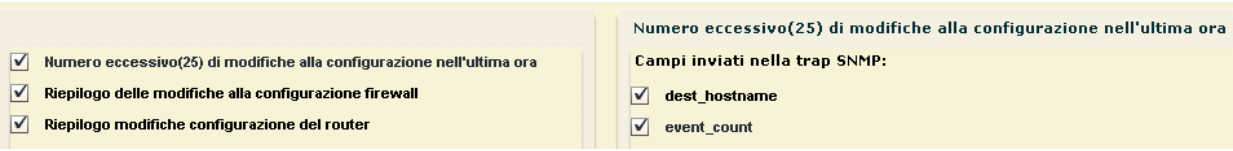


Nota: per impostazione predefinita, SpectroSERVER è in attesa sulla porta standard dei trap SNMP, ovvero la 162. Se modificata, la porta deve corrispondere al parametro snmp_trap_port del file SPECTRUM .vnmrc, che si trova nella directory SS.

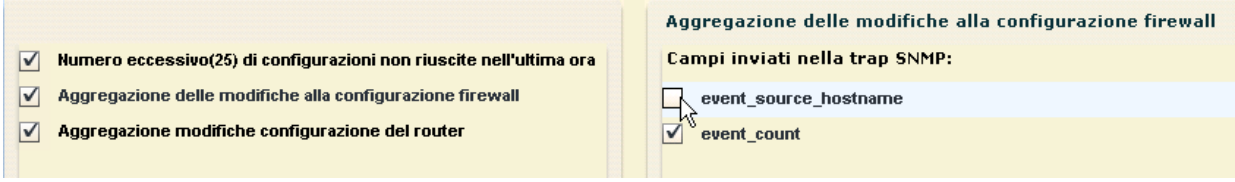
c. (Facoltativo). Per inviare il trap fino a nove server oltre al server di destinazione configurato, fare clic sul pulsante Aggiungi ed inserire l'indirizzo IP e la porta del server.

d. Se si desidera che una query specifichi l'inserimento di tutti i campi nel trap, selezionare la query.

Tutti i campi della query selezionata verranno selezionati per impostazione predefinita. Il nome della query selezionata verrà visualizzato in cima all'elenco dei campi.



e. Se si desidera che una query inserisca nel trap i campi selezionati, selezionare la query e deselezionare i campi da non inviare.



f. Selezionare la versione di SNMP supportata dalla destinazione dei trap selezionata per i trap ricevuti dalle applicazioni.

Nota: alcune destinazioni di trap accettano i trap di versione 3 inviati direttamente dai dispositivi, ma solo i trap di versione 2 da applicazioni che raccolgono gli eventi dai dispositivi. Per questo esempio, è accettata la versione 2.

5. Selezionare il server e specificare se la query dovrà restituire risultati solo dai server selezionati o da questo server e tutti i relativi server federati figli (se gerarchico) o peer (se a coppie).

6. Fare clic su Salva e chiudi.

   Il processo verrà visualizzato nell'elenco Processi di avviso. A meno che al primo passaggio della procedura guidata non sia stata deselezionata la casella di controllo Abilita, verrà visualizzato come Abilitato. Di seguito un semplice esempio:

Processi di avviso

	Nome processo	Abilitato	Server	Ricorrenza	Ora di inizio	Ora di fine	Fuso orario	Autore
	Configuration_Changes_Alert	true	ca-elm	5 minuti	Mercoledì 11/11/2009 24:56:08		America/New_York	su

Seguire l'avanzamento dei processi di avviso

È possibile visualizzare i risultati restituiti dalle query selezionate per gli avvisi creati dall'utente. I risultati visualizzati per l'esempio Configuration_Changes_Alert verranno visualizzati in CA User Activity Reporting Module sotto le intestazioni di host e conteggio.

1. Fare clic sulla scheda Gestione avvisi e quindi sulla sottoscheda Avvisi.
2. Fare clic sul nome dell'avviso pianificato.
3. Visualizzare i risultati per tale avviso.

   Seguono alcuni risultati di esempio:

Nome avviso	Categoria	Data
Configuration_Changes_Alert	Numero eccessivo(25) di modifiche alla configurazione nell'ultima ora	Giovedì 12/11/2009 16:09:28

Configuration_Changes_Alert

Alert name(Configuration_Changes_Alert) Alert created by(su) Federated job(Yes) Tags (Action Alerts)
Time Zone (America/New_York) Lists Excessive Configuration Changes (more than 25) in last hour.
Rows Returned(1)

Host	Conteggio
ca-elm	2

Visualizzare trap SNMP in CA Spectrum

È possibile visualizzare i trap SNMP inviati dagli avvisi CA User Activity Reporting Module nel modello eventi di CA Spectrum creato per riceverli. I trap ricevuti verranno visualizzati nella scheda Eventi. Per l'esempio Configuration_Changes_Alert, in CA Spectrum verranno visualizzati i risultati ca-elm e 2 con gli OID 1.3.6.1.4.1.791.9845.2.22 e 1.3.6.1.4.1.791.9845.2.2.

Per visualizzare trap SNMP in CA Spectrum

1. Accedere a CA Spectrum con le proprie credenziali.
2. Richiamare il Pannello di controllo di Spectrum ed avviare Spectroserver.

   Verrà avviato Spectroserver.
3. Fare clic su OneClick Administrator ed eseguire l'accesso.

   Verrà visualizzata l'applicazione Spectrum NFM OneClick.
4. Fare clic su Avvia console.

   Verrà visualizzata la console Spectrum OneClick.
5. Espandere la cartella creata per CA User Activity Reporting Module.
6. In Universe, selezionare il modello di evento creato per la ricezione dei trap inviati da CA User Activity Reporting Module.
7. Nel riquadro di destra, selezionare la scheda Eventi per visualizzare i trap inviati da CA User Activity Reporting Module.

   Il valore ca-elm ed event_count=2 corrispondono ai dati visualizzabili in CA User Activity Reporting Module.

Segue un esempio non correlato su come un trap SNMP inviato da un avviso di CA User Activity Reporting Module viene visualizzato in CA Spectrum OneClick. Il collegamento è l'URL che è possibile incollare in un browser per visualizzare la tabella di CA User Activity Reporting Module con le informazioni in formato CEG.

Evento

```
Trap 6.1 received from unknown SNMP device with IP address 155.35.29.12 and community string 'public'. Trap identifier 1.3.6.1.4.1.791.9845.3.
Trap var bind data:
OID: 1.3.6.1.2.1.1.3.0 Value: 30000
OID: 1.3.6.1.6.3.1.1.4.1.0 Value: 1.3.6.1.4.1.791.9845.3.1
OID: 1.3.6.1.4.1.791.9845.2.65 Value: Tue Sep 22 2009 01:32:30 PM
OID: 1.3.6.1.4.1.791.9845.2.44 Value: epSIM
OID: 1.3.6.1.4.1.791.9845.2.45 Value: etr851l1-blade7.ca.com
OID: 1.3.6.1.4.1.791.9845.2.77 Value: Unknown Category
OID: 1.3.6.1.4.1.791.9845.2.75 Value: Unknown Action
OID: 1.3.6.1.4.1.791.9845.2.81 Value: Success
OID: 1.3.6.1.4.1.791.9845.4.1 Value:
https://etr851l1-blade7.ca.com:5250/spin/calmapi/getObject.csp?type=getQueryViewer&objectId=Subscription/panels/System_All_Events_Detail&params=
;Params><Param id="ARG_stop" val="1253606639,'unixepoch'"/><Param id="ARG_start" val="1253606339,'unixepoch'"/><Param id="ARG_localtimezone
val="Asia/Calcutta"/></Params>
```

Ulteriori informazioni:

Esempio: avvisare CA Spectrum delle modifiche alla configurazione (a pagina 451)

Preparazione di CA NSM per la ricezione di trap SNMP dagli avvisi

È possibile inviare gli avvisi sottoforma di trap SNMP da CA User Activity Reporting Module a qualsiasi destinazione della rete in grado di ricevere ed interpretare le trap. Ogni prodotto che riceve trap possiede i propri requisiti.

Preparare CA NSM alla ricezione di trap a partire dagli avvisi mediante le seguenti operazioni:

- Verificare che il sistema CA NSM di destinazione soddisfi i requisiti di sistema per la ricezione dei dati di trap SNMP da CA User Activity Reporting Module.
- Configurare CA NSM per la ricezione di trap SNMP, abilitare il supporto per SNMP v3, modificare l'assegnazione delle porte nei vari file ed avviare i servizi richiesti.

Preparare CA NSM per interpretare le trap ricevute dagli avvisi attenendosi alle procedure descritte di seguito:

- Creare una MIB personalizzata per ciascun avviso che si desidera inviare come una trap SNMP a CA NSM.
- Importare e compilare il file CA-ELM.MIB e tutte le MIB personalizzate.

Requisiti di sistema di CA NSM

È possibile inviare trap SNMP a CA NSM se il sistema in uso soddisfa i seguenti requisiti di interfaccia di CA User Activity Reporting Module:

- La versione di CA NSM è CA NSM r12.2 (build GA).
- CA NSM è installato in Windows Server 2003 EE SP1.
- È applicata la patch T5MK056.caz, che aggiorna il file aws_snmpex.dll, consentendo a CA NSM di ricevere trap SNMP v3 da CA User Activity Reporting Module.

Per applicare la patch

1. Scaricare la patch dal sito del supporto tecnico di CA.
2. Accedere al server con CA NSM.

3. Arrestare il servizio Trap SNMP:
   a. Dal menu Start, selezionare Programmi, Strumenti di amministrazione, Servizi.

      Verrà visualizzato l'elenco Servizi.

   b. Selezionare il servizio Trap SNMP, fare clic con il pulsante destro del mouse e selezionare Interrompi dal menu visualizzato.
4. Arrestare tutti i servizi CA NSM:
   a. Accedere al prompt dei comandi.
   b. Immettere il seguente comando:

      ```
      Unicntrl stop all
      ```
5. Copiare il file di download della patch, "T5MK056.caz", nella cartella C:\temp.
6. Decomprimere il file della patch con cazipxp.

   ```
   Cazipxp.exe –u T5MK056.caz
   ```
7. Fare una copia di backup del file aws_snmpex.dll esistente prima di sostituirlo.
   a. Accedere al percorso C:\Program Files\CA\SC\CCS\AT\SERVICES\BIN.
   b. Fare clic con il pulsante destro del mouse su aws_snmpex.dll e selezionare Copia.

      Verrà aggiunta una copia di aws_snmpex.dll alla cartella.
8. Copiare aws_snmpex.dll dalla cartella temp alla cartella bin (C:\Program Files\CA\SC\CCS\AT\SERVICES\BIN)

   A questo punto, CA NSM soddisferà i requisiti di sistema. È possibile configurare CA NSM per la ricezione di trap SNMP da CA User Activity Reporting Module.

Configurare CA NSM per la ricezione di trap SNMP

Per poter indirizzare gli avvisi da inviare a CA NSM come trap SNMP, è necessario configurare CA NSM per la ricezione di trap. È possibile inviare a CA NSM sia trap SNMP v3 che v2.

Per configurare CA NSM per la ricezione di trap SNMP dagli avvisi di CA User Activity Reporting Module

1. Accedere a CA NSM.
2. Abilitare il supporto per SNMP versione 3 come segue:
   a. Aprire il prompt dei comandi. Dal menu Start, fare clic su Esegui, digitare cmd e fare clic su OK.
   b. Digitare la seguente stringa:

      ```
      caugui settings
      ```

      Viene visualizzata la finestra Impostazioni EM.
   c. Fare clic sulla scheda Gestione avvisi.
   d. Scorrere per visualizzare la descrizione: SNMP - Abilitare il supporto a SNMP versione 3.
   e. Selezionare la riga e digitare Y per selezionare YES nella colonna delle impostazioni per SNMP Abilitare il supporto per SNMP versione 3.
   f. Fare clic su Yes per confermare l'eliminazione.
   g. Chiudere la finestra.
3. Modificare la porta utilizzata dal servizio SNMP, passando dalla porta attuale, ad esempio 5162, alla porta 162 come segue:
   a. Aprire Esplora risorse.
   b. Accedere alla cartella .../System32/drivers/etc, solitamente disponibile in C:\WINDOWS.
   c. Eseguire il backup del file Servizi. Fare clic con il pulsante destro del mouse su Servizi e scegliere Copia.

d. Aprire il file Servizi in un editor di testo, come il Blocco Note, e scorrere fino alla voce analoga alla seguente:

```
snmptrap      162/udp     snmp-trap    #SNMP trap
```

e. Modificare la riga snmptrap per sostituire il numero di porta 162 con un'alternativa, ad esempio 5162. Aggiungere la riga catrapmuxd in cui assegnare la porta 162.

```
snmptrap     5162/udp
catrapmuxd    162/udp     catrapmuxd  #CA Trap Multiplexer
```

f. Salvare e chiudere il file.

4. Modificare il file di configurazione di CA Trap Multiplexer, catrapmux.conf, come segue:

   a. Accedere al percorso C:\Programmi\CA\SC\CCS\WVEM\CAIUSER.

   b. Aprire il file CATRAPMUX.CONF in un editor di testo, come il Blocco note.

   c. Scorrere fino alla fine del file. Modificare il file inserendo le seguenti voci.

```
CATRAPMUX_CMD:6161
AWS_SNMP:6162
catrapd:6163
snmptrap:5162
```

   Nota: le prime tre voci rappresentano le impostazioni predefinite.

   d. Salvare e chiudere il file.

5. Aggiungere una riga al file di configurazione snmpv3.dat in modo da configurare i parametri di sicurezza di SNMP v3.

   a. Accedere al percorso C:\Programmi\CA\SC\CCS\CommonResourcePackages\CAIUSER.

   b. Aprire snmpv3.dat in un editor di testo ed aggiungere la seguente riga alla fine del file.

```
*.*.*.* *:*                    test1234:AuthPriv:MD5:test1234:DES:test1234
```

   Nota: si tratta degli stessi parametri da inserire nella finestra Parametri di protezione V3 di SNMP della procedura guidata Avviso per fare in modo che CA NSM possa ricevere il trap SNMP. Il nome utente e la password sono quelli configurati in questa sede, il protocollo Auth è MD5 ed il protocollo di crittografia è DES.

   c. Salvare e chiudere il file.

6. Installare il servizio CA Trap Multiplexer:
   a. Accedere al prompt dei comandi.
   b. Immettere il seguente comando:

      ```
      catrapmuxd uniconfig
      ```

      CA Trap Multiplexer verrà aggiunto all'elenco Servizi con lo stato Avviato.
7. Verificare che CA Trap Multiplexer sia in esecuzione ed avviare il servizio trap SNMP.
   a. Dal menu Start, selezionare Programmi, Strumenti di amministrazione, Servizi.

      Verrà visualizzato l'elenco Servizi.
   b. Osservare lo stato di CA Trap Multiplexer. Verificare che lo Stato sia Avviato.
   c. Selezionare il servizio Trap SNMP, fare clic con il pulsante destro del mouse e selezionare Avvia dal menu di scelta rapida.
8. Avviare tutti i servizi con tipo di avvio Automatico.
   a. Accedere al prompt dei comandi.
   b. Immettere il seguente comando:

      ```
      Unicntrl stop all
      ```

   CA NSM verrà configurato per la ricezione di trap SNMP v3 in base agli avvisi pianificati inviati da CA User Activity Reporting Module.

Esempio: Segnalazione di modifiche della configurazione a CA NSM

L'esempio seguente è progettato per guidare l'utente attraverso un processo di segnalazione di modifiche della configurazione a CA NSM. Il processo prevede le seguenti procedure:

- Invio di trap SNMP a CA NSM
- Verifica dell'invio di trap SNMP
- Accesso alla console EM in CA NSM
- Visualizzazione delle trap SNMP ricevute da CA NSM

Invio delle trap SNMPv3 a CA NSM

Durante la pianificazione degli avvisi da inviare a CA NSM, identificare i risultati di query che potrebbero essere di interesse per il centro delle operazioni di rete. Ad esempio, prendere in considerazione query che rilevano le modifiche di configurazione. Il seguente esempio descrive la modalità di invio di un avviso pianificato in base alla query dei dettagli di modifica della configurazione. L'avviso specifica CA NSM come destinazione di trap SNMP.

Per inviare le trap SNMPv3 a CA NSM

1. Aprire la procedura guidata Pianificazione avvisi.
   a. Accedere a CA User Activity Reporting Module con le credenziali di analista o amministratore.
   b. Fare clic sulla scheda Gestione avvisi, quindi sulla sottoscheda Pianificazione avvisi.
   c. Fare clic sul pulsante Pianifica un avviso.
2. Eseguire il passaggio Selezione avviso.
   a. Inserire un nome processo. Ad esempio, inserire Modifiche di configurazione destinate a CA NSM.
   b. Verificare che il tipo di selezione corrisponda a Query. Non è consentito selezionare le destinazioni di trap SNMP per gli avvisi basati sui tag.
   c. Selezionare la query o le query identificate. Ad esempio, selezionare i dettagli di modifica della configurazione.
3. (Facoltativo) Eseguire i passaggi Filtri di avviso, Condizioni di risultato e Pianifica processi, come documentato nella Guida in linea per questa procedura guidata.
4. Fare clic sul passaggio Destinazione, quindi sulla scheda trap SNMP.
5. Esaminare le voci di server e porta di destinazione. Se non sono corrette, inserire il corretto indirizzo IP del server di destinazione e la porta. Per aggiungere ulteriori server di destinazione, fare clic su Aggiungi ed inserire le destinazioni aggiuntive.

6. Specificare la versione di SNMP. Il protocollo SNMP versione 2 è selezionato per impostazione predefinita.

   a. Fare clic su Versione 3. CA NSM è configurato per accettare le trap SNMP v3.

   b. Fare clic su Protezione V3.

      Verrà visualizzata la finestra Parametri di protezione di SNMP versione 3.

      Importante: le voci di questa finestra devono corrispondere alle impostazioni del file snmpv3.dat, configurato per abilitare CA NSM alla ricezione di trap SNMP dagli avvisi di CA User Activity Reporting Module. Seguono le impostazioni consigliate:

      ```
      *.*.*.* *:*   <nomeutente>:AuthPriv:MD5:<password>:DES:<password>
      ```

   c. Selezionare Autenticazione. Digitare il nome utente configurato come nome utente, digitare la password configurata come password e selezionare MD5 come protocollo.

   d. Selezionare Crittografia. Digitare la password configurata e selezionare DES come protocollo.

   e. Fare clic su OK.

7. Selezionare la query da inviare come trap SNMP.

   In questo esempio, selezionando Dettagli di modifica configurazione, i campi per tale query verranno visualizzati come selezionati. Facoltativamente, è possibile cancellare i campi che non si desidera inserire come trap.

   Importante: durante la creazione di una MIB personalizzata per l'avviso, accertarsi di definire una trap con i campi selezionati nell'ordine visualizzato.

8. Selezionare il numero del nodo finale, x, dell'OID elmTrap associato, in cui tutti gli OID elmTrap sono definiti come 1.3.6.1.4.1.791.9845.3.x.

   I nodi iniziali dell'ID di trap personalizzato sono predefiniti nel file CA-ELM.MIB. Il numero del nodo finale è univoco per una trap definita in una MIB personalizzata, in cui la trap rappresenta un set di campi univoco. Un file MIB personalizzato determina le trap inviate dagli avvisi di CA User Activity Reporting Module definiti dall'utente. Nella trap personalizzata identificata dell'ID di trap personalizzato, i campi vengono elencati nello stesso ordine di quelli inviati dall'avviso. Se l'OID della trap nella MIB personalizzata corrisponde a 1.3.6.1.4.1.791.9845.3.63, selezionare 63 dalla casella di selezione per l'ID di trap personalizzato. Se si desidera definire prima l'avviso, aggiungere una trap nella MIB personalizzata per 1.3.6.1.4.1.791.9845.3.63. In tal modo, vengono definiti i campi di query selezionati.

9. (Facoltativo) Selezionare server.

10. Fare clic su Salva, quindi su Chiudi.

    Il processo verrà visualizzato nell'elenco Processi di avviso, con il nome di processo configurato.

Ulteriori informazioni:

Accedere alla console EM su CA NSM (a pagina 465)

Seguire l'avanzamento dei processi di avviso

Quando si pianifica un avviso, è consigliabile seguire l'avanzamento della prima esecuzione del processo di avviso. Nel seguire l'avanzamento è possibile verificare l'effettiva esecuzione del processo e la correttezza dei risultati di rapporto rispetto a quanto era previsto per l'invio.

Per monitorare l'avanzamento del processo di avviso e visualizzare in anteprima i risultati

1. All'interno dell'elenco Processi di avviso, visualizzare il processo di avviso creato dall'utente. Segue un esempio parziale:

Processi di avviso

	Nome processo	Abilitato	Server	Ricorrenza	Ora di inizio
	Configuration Changes destined for CA	true	etr851l1-blade3	5 minuti	Lunedì 07/12/2009 19:13:30

2. (Facoltativo) Per seguire l'avanzamento del processo di avviso, visualizzare Dettagli eventi di automonitoraggio di sistema. Fare doppio clic su qualsiasi riga per aprire il Visualizzatore eventi. Scorrere fino a result_string per visualizzare l'intero messaggio presente in Descrizione risultato.

Azione	Risultato	Descrizione risultato
Notification Creation	S	SNMP trap for Action Query [Configuration Change Detail] Alert Name [Configuration Changes destined for CA NSM] on report:
Resource Creation	S	Creation of job file while executing action alert for Alert Name [Configuration Changes destined for CA NSM] was Successful.
Alert Creation	S	Run Action Query [Configuration Change Detail] Alert Name [Configuration Changes destined for CA NSM] on reportServer [etr
Resource Modify	S	Update RSSFeed Alert Name [Configuration Changes destined for CA NSM] on reportServer [etr6511l1-sun104] recurrence [5
Resource Execution	S	Query [Configuration Change Detail] run over logDepot [localhost] was successful .

3. Visualizzare l'anteprima dei risultati restituiti dalle query selezionate per l'avviso creato dall'utente.

   a. Fare clic sulla scheda Gestione avvisi e quindi sulla sottoscheda Avvisi.

   b. Fare clic sul nome dell'avviso pianificato.

   c. Visualizzare i risultati per tale avviso.

   Nota: di solito, qui vengono visualizzati gli stessi dati ottenuti aprendo l'URL inviato al server di destinazione. Nel caso in cui siano presenti differenze, per fare in modo che i risultati siano uguali occorre modificare l'avviso in modo da reimpostare l'ora di fine dinamica per le Condizioni di risultato. Ad esempio, impostarla su "ora", "-10 minuti".

Accedere alla console EM su CA NSM

È possibile visualizzare i trap SNMP inviati da CA User Activity Reporting Module da CA NSM. Sulla console EM, i trap SNMP vengono visualizzati come messaggi.

Accedere alla console EM su CA NSM

1. Accedere al server in cui è installata la destinazione dei trap SNMP, CA NSM.
2. Dal menu Start, selezionare Programmi, CA, Unicenter, NSM, Enterprise Management ed EM Classic.

   Verrà visualizzata la finestra EM di Windows.
3. Fare doppio clic su Windows.

   Verrà visualizzata la finestra <nomehost> (Windows).
4. Fare doppio clic su Evento.

   Verrà visualizzata la finestra Evento <nomehost> (Windows).
5. Fare doppio clic sui registri delle console.

   Verrà visualizzata la console EM (<nomehost>).

Ulteriori informazioni:

Visualizzare i trap SNMP in CA NSM (a pagina 466)

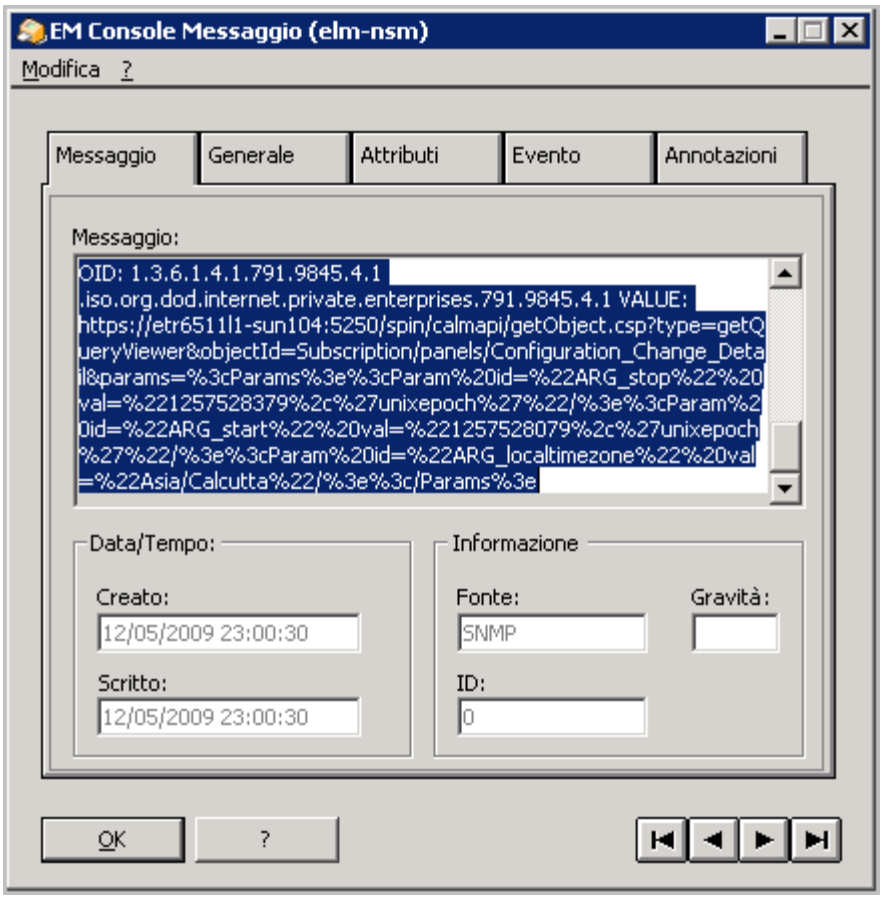
Visualizzare i trap SNMP in CA NSM

Si consideri l'esempio in cui un avviso viene pianificato per l'esecuzione della query Dettagli di modifica configurazione. In questa situazione, l'ID del trap personalizzato è impostato su 1,3.6,1.4,1.791,9845.3,63. Nove campi saranno inviati come trap SNMP.

Per visualizzare il trap SNMP inviato da un Avviso basato sulla query Dettagli di modifica configurazione

1. Quando un evento di automonitoraggio indica che un trap SNMP è stato inviato correttamente a CA NSM, accedere alla console EM su CA NSM.
2. Attendere fino a quando viene visualizzato un messaggio di registro che indica la ricezione di un trap SNMP. Il messaggio per questo trap contiene l'ID del trap personalizzato, 1,3.6,1.4,1.791,9845.3,63.

3. Fare doppio clic su questo messaggio per visualizzarlo in un formato che è possibile copiare.



4. Copiare il messaggio e incollarlo in un file di testo temporaneo.

   I risultati che si ottengono sono simili ai seguenti:

   ```
   %CATD_I_060, SNMPTRAP: -u auth user 791 155.35.7.63 etr6511l1-sun104.ca.com 6
   63 0:05:00 12
   ```

   Specifica la ricezione dei dati successivi come trap SNMP.

   ```
   OID: 1,3.6,1.2,1.1,3.0 system.sysUpTime.0 VALUE: (30000) 0:05:00,00
   ```

   Specifica l'ID dell'oggetto per il tempo di attività in centesimi di secondo. Si tratta di un ID oggetto noto attraverso SNMP.

```
OID: 1,3.6,1.6,3.1,1.4,1.0 .iso.org.dod.internet.snmpV2.snmpModules.1,1.4,1.0
VALUE: 1,3.6,1.4,1.791,9845.3,63
```

Specifica l'ID oggetto per l'snmpTrapOID. Il valore è l'ID del trap personalizzato specificato durante la configurazione dell'avviso.

```
OID: 1,3.6,1.4,1.791,9845.2,80
.iso.org.dod.internet.private.enterprises.791,9845.2,80 VALUE: 2
```

Specifica l'ID oggetto per event_severity e il valore di gravità 2, che sta per Informativo.

```
OID: 1,3.6,1.4,1.791,9845.2,65
.iso.org.dod.internet.private.enterprises.791,9845.2,65 VALUE: Fri Nov 06
2009 22:53:53
```

Specifica l'ID oggetto per event_datetime con il valore, il giorno, la data e l'ora in cui si è verificato l'evento con questi valori.

```
OID: 1.3.6.1.4.1.791.9845.2.17
.iso.org.dod.internet.private.enterprises.791.9845.2.17 VALUE:
```

Specifica l'ID oggetto per dest_username senza valori.

```
OID: 1.3.6.1.4.1.791.9845.2.1
.iso.org.dod.internet.private.enterprises.791.9845.2.1 VALUE:
```

Specifica l'ID oggetto per source_username senza valori.

```
OID: 1.3.6.1.4.1.791.9845.2.22
.iso.org.dod.internet.private.enterprises.791.9845.2.22 VALUE: etr851l2-elm5
```

Specifica l'ID oggetto per dest_hostname con il nome host del server in cui i risultati della query vengono visualizzati quando si avvia l'URL.

```
OID: 1.3.6.1.4.1.791.9845.2.53
.iso.org.dod.internet.private.enterprises.791.9845.2.53 VALUE: EiamSdk
```

Specifica l'ID oggetto per event_logname, EiamSdk, il nome del file di registro contenente questi dettagli.

```
OID: 1.3.6.1.4.1.791.9845.2.77
.iso.org.dod.internet.private.enterprises.791.9845.2.77 VALUE: Configuration
Management
```

Specifica l'ID oggetto per event_category e il valore per Categoria associati alla query Dettagli di modifica configurazione.

```
OID: 1.3.6.1.4.1.791.9845.2.75
.iso.org.dod.internet.private.enterprises.791.9845.2.75 VALUE: Configuration
Change
```

Specifica l'ID oggetto per event_action e il valore per Azione associati alla query Dettagli di modifica configurazione.

```
OID: 1.3.6.1.4.1.791.9845.2.81
.iso.org.dod.internet.private.enterprises.791.9845.2.81 VALUE: S
```

Specifica l'ID oggetto per event_result con il valore S, che indica Success.

```
OID: 1.3.6.1.4.1.791.9845.4.1
.iso.org.dod.internet.private.enterprises.791.9845.4.1 VALUE:
https://etr6511l1-
sun104:5250/spin/calmapi/getObject.csp?type=getQueryViewer&objectId=Subscript
ion/panels/Configuration_Change_Detail&params=%3cParams%3e%3cParam%20id=%22AR
G_stop%22%20val=%221257528379%2c%27unixepoch%27%22/%3e%3cParam%20id=%22ARG_st
art%22%20val=%221257528079%2c%27unixepoch%27%22/%3e%3cParam%20id=%22ARG_local
timezone%22%20val=%22Asia/Calcutta%22/%3e%3c/Params%3e
```

Specifica l'ID oggetto per calmAPIURL sotto elmDynamicVariables. Il valore è l'URL di CA User Activity Reporting Module API. Dopo aver eseguito l'accesso, è possibile visualizzare i risultati della query in formato grafico o di diagramma.

5. Copiare l'URL in fondo al messaggio, incollarlo in un browser ed aprirlo.
6. Accedere a CA User Activity Reporting Module API.

   Viene visualizzata la vista a diagramma Dettagli di modifica configurazione Consultare l’esempio seguente:

Creazione di un alert

Il processo per la creazione di un avviso tramite la procedura guidata Pianifica alert è composto dai seguenti passaggi:

1. Aprire la procedura guidata Pianifica alert.
2. Scegliere la query o i tag anche su cui si basa l'avviso. È possibile eseguire una query sul database eventi, sul database incidenti o su entrambi in un unico processo.
3. (Facoltativo) Impostazione di filtri avanzati per definire ulteriormente la query di avviso.
4. (Facoltativo) Impostare l'intervallo di data e le condizioni di risultato
5. (Facoltativo) Definizione della frequenza di ricorrenza del processo di avviso e della sua attivazione.
6. (Facoltativo) Configurare i messaggi di posta elettronica ed i destinatari degli avvisi automatici.
7. (Facoltativo) Esecuzione della query soltanto per i dati del server selezionato oppure per il server e gli elementi figlio corrispondenti.

   Nota: un alert non può basarsi su una query ODBC.

Ulteriori informazioni:

Apertura della procedura guidata di pianificazione di avvisi (a pagina 471)
Creazione di un filtro di eventi avanzato (a pagina 586)
Impostare le destinazioni di notifica (a pagina 474)
Definizione della destinazione della query del processo di avviso (a pagina 479)

Apertura della procedura guidata di pianificazione di avvisi

Per creare un processo di avviso, è necessario utilizzare la procedura guidata di pianificazione di avvisi.

Per aprire la procedura guidata di pianificazione di avvisi

1. Fare clic sulla scheda Gestione avvisi.

   Viene visualizzato l'elenco dei server avvisi.

2. Selezionare il server sul quale si desidera pianificare un avviso.

   Il pannello Dettagli server mostra il server selezionato e, per impostazione predefinita, la scheda degli avvisi generati.

3. Fare clic sulla scheda Pianificazione avvisi, quindi sul pulsante Pianifica avviso.

   Viene visualizzata la procedura guidata di pianificazione di avvisi.

   Mentre si utilizza la procedura guidata:

   - Fare clic su Salva e chiudi per salvare l'avviso e chiudere la procedura.
   - Fare clic su Ripristina per ripristinare la visualizzazione della procedura alle ultime impostazioni salvate.

Ulteriori informazioni

Impostazione della destinazione delle notifiche tramite posta elettronica (a pagina 475)
Definizione della destinazione della query del processo di avviso (a pagina 479)

Selezione di una query di avviso

Selezione di tag o query come base per un nuovo processo di avviso. La query, con i filtri aggiunti dall'utente, definisce le circostanze in cui si genera un avviso. Ad esempio, per creare un avviso per monitorare il traffico da un host o da una porta, usare la query Tutti gli eventi, aggiungere i filtri per definire gli host di origine da monitorare e una soglia eventi.

Nota: la categoria query Avvisi contiene query concepite per varie esigenze comuni degli avvisi.

Per selezionare una query di avviso

1. Aprire la procedura guidata per gli avvisi pianificati.
2. Inserire un nome processo.
3. Selezionare il fuso orario in cui si desidera pianificare il rapporto dal menu a discesa dei fusi orari.
4. Selezionare il pulsante Query o Tag per selezionare i rapporti in base al tag o individualmente.

   Nota: la pianificazione degli avvisi per tag consente di aggiungere avvisi senza alterare il processo stesso. Se si seleziona il tag "Gestione identità", qualsiasi avviso con tale tag viene aggiunto al processo all'ora di avvio pianificata. È possibile aggiungere un nuovo avviso al processo assegnando a una query il tag Gestione identità. Questa caratteristica si applica anche ai tag personalizzati.

   (Facoltativo) Deselezionare la casella di controllo Attiva per abilitare l'avviso successivamente invece che subito. La casella è selezionata per impostazione predefinita.

   Nota: la possibilità di creare un processo di avviso disabilitato è progettata per l'uso con i rapporti ricorrenti. Deselezionando la casella di controllo Attiva per un processo e creando tale processo con una singola occorrenza ("Ora" o "Una volta"), il processo viene rimosso dall'elenco Avvisi pianificati.
5. (Facoltativo) Selezionare un tag o più tag per restringere il numero di tag e rapporti individuali selezionati. Questa caratteristica corrisponde al comportamento dell'Elenco rapporti.
6. Selezionare i tag o le singole query da utilizzare come modello e aggiungerli tramite il controllo pilota all'area Query selezionate. È possibile selezionare in un singolo processo di avviso sia query di evento che query di incidente.
7. Procedere con il passaggio di pianificazione che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

Facendo clic su Salva e chiudi, il processo di avviso viene pianificato; altrimenti, verrà visualizzato il passaggio selezionato.

Ulteriori informazioni:

Creazione di un filtro di eventi avanzato (a pagina 586)

Impostazione dei parametri di pianificazione di un processo di avviso

È possibile controllare il momento in cui gli avvisi vengono applicati impostandone l'ora di inizio e di fine. È inoltre possibile controllare la granularità della visualizzazione degli avvisi tramite la verifica della frequenza di ricorrenza della query.

Per impostare i parametri di pianificazione dei processi di avviso

1. Aprire la procedura guidata Pianifica avviso e inserire le informazioni richieste; quindi, proseguire con il passaggio Pianifica processi.
2. Impostare l'intervallo di ricorrenza desiderato. Un intervallo più basso consente una visualizzazione più dettagliata, ma aumenta il traffico di rete.

   Prima di impostare un intervallo basso, verificare la sincronizzazione di CA User Activity Reporting Module con un server NTP.
3. Impostare la data di inizio e di fine desiderata per il processo di avviso.
4. Procedere con il passaggio di pianificazione che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, il processo di avviso viene pianificato; altrimenti, verrà visualizzato il passaggio selezionato.

Impostare le destinazioni di notifica

È possibile impostare una o più delle seguenti destinazioni per la notifica di un avviso:

- Posta elettronica

  È possibile impostare la notifica automatica di un avviso tramite posta elettronica, in modo da garantire che il personale interessato riceva gli avvisi relativi al ruolo o alle responsabilità ricoperte nell'ambito del processo. Configurare un server di posta per l'ambiente CA User Activity Reporting Module in uso prima di inviare messaggi di posta elettronica con notifica di avviso.

- Processo CA IT PAM

  È possibile eseguire il processo CA IT PAM specificato se l'avviso dipende da una condizione che richiede la notifica del prodotto di terze parti. È necessario configurare l'integrazione con CA IT PAM in Server di rapporto, definendo il processo di CA IT PAM prima di poterlo eseguire a partire dagli avvisi.

- Trap SNMP

  È possibile inviare i dati di evento acquisiti da un avviso a uno o più centri delle operazioni di rete. È possibile impostare come destinazione server di gestione come CA Spectrum o CA NSM che utilizzano trap SNMP v2 o v3. Specificare le destinazioni in fase di pianificazione dell'avviso. È necessario configurare l'integrazione con SNMP per poter utilizzare avvisi sfruttando tale protocollo.

Nota: se non si imposta una destinazione, i risultati di avviso saranno pubblicati solo sul feed RSS.

Ulteriori informazioni:

Impostazione della destinazione delle notifiche tramite posta elettronica (a pagina 475)
Impostare le informazioni di CA IT PAM (a pagina 476)
Esempio: avvisare CA Spectrum delle modifiche alla configurazione (a pagina 451)
Esempio: inviare un avviso che esegue un processo IT PAM per riga (a pagina 415)
Esempio: inviare un avviso che esegua un processo di IT PAM per query (a pagina 420)

Impostazione della destinazione delle notifiche tramite posta elettronica

È possibile impostare la notifica automatica tramite posta elettronica di un processo di avviso, in modo da garantire che il personale interessato riceva gli avvisi relativi al ruolo o alle responsabilità ricoperte nell'ambito del processo. Questo passaggio è facoltativo.

Prima di poter impostare i messaggi di notifica di avviso, è necessario configurare un server di posta elettronica per il proprio ambiente CA User Activity Reporting Module.

Per impostare notifiche di avviso

1. Aprire la procedura guidata di pianificazione avviso, inserire le informazioni richieste e avanzare al passaggio Destinazione.
2. Selezionare la casella di controllo Attiva notifica tramite posta elettronica.
3. Inserire almeno un indirizzo di posta elettronica destinatario. È possibile inserire più indirizzi separati da virgole.
4. (Facoltativo) Inserire il mittente, una riga per l'oggetto e un corpo del messaggio per la notifica tramite posta elettronica.

   Nota: il corpo del messaggio è in formato HTML, pertanto il testo inserito verrà visualizzato su un'unica riga. Per creare un'interruzione dopo una riga, inserire <BR/> alla fine della riga di testo.

Ulteriori informazioni:

Impostare le informazioni di CA IT PAM (a pagina 476)

Impostare le informazioni di CA IT PAM

È possibile impostare il processo di avviso in modo da eseguire un processo CA IT PAM quando l'avviso viene generato.

È possibile eseguire il processo una volta per ogni riga di risultati della query, oppure eseguire il processo configurato una volta sola, indipendentemente dal numero di righe. Se si esegue il processo una volta per riga, definire le istruzioni di riepilogo e descrizione utilizzando i campi CEG per trasmettere i dati di evento a CA IT PAM. Selezionare i campi definiti per raccogliere i dati per la query. Se si esegue il processo una volta per query, verrà trasmesso automaticamente un URL a CA IT PAM che, una volta avviato, visualizzerà tutte le righe dei dati di evento. Nel prodotto di terze parti che risponde al processo di CA IT PAM, l'URL verrà aggiunto al testo di riepilogo inserito dall'utente. Ad esempio, verrà visualizzato nel campo Riepilogo di CA Service Desk, se quest'ultimo è il prodotto di terze parti.

Per eseguire un processo di CA IT PAM quando viene generato l'avviso

1. Aprire la procedura guidata di pianificazione avviso, inserire le informazioni richieste e avanzare al passaggio Destinazione.
2. Fare clic sulla scheda Processo CA IT PAM.

   Nel riquadro di sinistra verrà visualizzata una casella di controllo per ogni query di questo processo di avviso.
3. Selezionare la query che si desidera inviare al processo CA IT PAM ed eseguire una delle seguenti azioni:
   - Selezionare Eseguire il processo CA IT PAM per riga per eseguire il processo configurato una volta per ogni riga restituita.
   - Deselezionare Eseguire il processo CA IT PAM per riga per eseguire il processo configurato una sola volta, indipendentemente dal numero di righe restituite.
4. Verificare le voci predefinite per i parametri di processo e modificarle, se necessario. Per i campi non definiti che consentono di inserire informazioni di riepilogo e descrizione, immettere un'istruzione significativa. Se si seleziona Eseguire il processo CA IT PAM per riga, utilizzare i campi CEG per trasmettere i dati di evento. Selezionare il campo CEG e fare clic su Aggiungi accanto al campo di destinazione.
5. Se il processo CA IT PAM viene definito con i campi CEG come parametri locali nel dataset, selezionare tali campi nell'elenco Invia valori campo come parametri.

6. Selezionare un'altra query dal riquadro di sinistra e ripetere i passaggi da 3 a 6.

Nota: quando le query per un processo di avviso pianificato restituiscono risultati, tutte le informazioni ed i parametri necessari per eseguire il processo configurato verranno inviati a CA IT PAM.

Ulteriori informazioni:

Impostazione della destinazione delle notifiche tramite posta elettronica (a pagina 475)

Impostare le informazioni di trap SNMP

È possibile impostare le informazioni di trap SNMP per un processo di avviso, allo scopo di inviare l'avviso ad uno o più sistemi di gestione di terze parti. Quando le query selezionate restituiscono risultati, un trap contenente i dati restituiti per tutti i campi selezionati di tutte le query selezionate verrà inviato a tutte le destinazioni di trap SNMP selezionate. Questo passaggio è facoltativo.

Per impostare le informazioni dei trap SNMP

1. Aprire la procedura guidata di pianificazione avviso, inserire le informazioni richieste e avanzare al passaggio Destinazione.
2. Selezionare la scheda Trap SNMP.

   Verrà visualizzata la scheda trap SNMP contenente i campi Server di destinazione e Porta di destinazione ed un elenco delle query inserite in Avvisi, ognuna con una casella di controllo.
3. Esaminare le voci predefinite di server e porta di destinazione. Se non sono corrette, inserire l'indirizzo IP corretto oppure il nome di host completo ed il numero di porta.
4. (Facoltativo) Fare clic su Aggiungi per inserire porte e server di destinazione aggiuntivi.
5. (Facoltativo) Per inviare l'avviso utilizzando SNMP v3, selezionare SNMP versione 3. L'impostazione predefinita è SNMP versione 2.
6. Se si seleziona SNMP versione 3, fare clic sul pulsante Protezione V3 per impostare l'autenticazione o la crittografia nella finestra Parametri di protezione.

Importante: le voci di questa finestra devono corrispondere alle impostazioni del file snmpv3.dat, configurato per abilitare CA NSM alla ricezione di trap SNMP dagli avvisi di CA User Activity Reporting Module. Seguono le impostazioni consigliate:

```
*.*.*.* *:*   <nomeutente>:AuthPriv:MD5:<password>:DES:<password>
```

a. Selezionare Autenticazione. Digitare il nome utente configurato come nome utente, digitare la password configurata come password e selezionare MD5 come protocollo.

b. Selezionare Crittografia. Digitare la password configurata e selezionare DES come protocollo.

7. Selezionare la casella di controllo accanto ad una qualsiasi query da inserire nel trap SNMP. Ad esempio, se nell'elenco sono presenti tre query, è possibile impostare SNMP per inviarne una, due o tutte e tre.

   Scegliendo una query verranno visualizzati i campi compresi in ogni query, con una casella selezionata. È possibile deselezionare un campo selezionato per eliminarlo dall'avviso.

8. Immettere l'ID trap personalizzato associato ad ogni query. Ciò consente, se necessario, di inviare query diverse in un unico avviso ad ID trap diversi.

9. Procedere con il passaggio di pianificazione che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Facendo clic su Salva e chiudi, il processo di avviso viene pianificato; altrimenti, verrà visualizzato il passaggio selezionato.

Ulteriori informazioni:

Impostazione della destinazione delle notifiche tramite posta elettronica (a pagina 475)
Impostare le informazioni di CA IT PAM (a pagina 476)

Definizione della destinazione della query del processo di avviso

È possibile scegliere quali archivi registro eventi federati verranno interrogati dal processo di avviso.

Per scegliere le destinazioni del rapporto

1. Aprire la procedura guidata di pianificazione di avvisi, inserire le informazioni richieste e proseguire con il passaggio Selezione server.
2. Selezionare gli eventuali server disponibili cui si vuole indirizzare la query e trasferirli nell'area Server selezionati utilizzando il controllo pilota.
3. (Facoltativo) Per disabilitare le query federate per questo processo di avviso, selezionare "No" dal menu a discesa che appare quando si fa clic sulla voce Query federate. Le query dei rapporti sono federate per impostazione predefinita.
4. Procedere con il passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, il processo di avviso viene pianificato; altrimenti, verrà visualizzato il passaggio selezionato.

Esempio: creazione di un avviso per Spazio su disco insufficiente

Spazio su disco insufficiente è una delle query predefinite con il tag Avvisi. Le query con il tag Avvisi sono concepite specificamente per essere usate come avvisi, ma non lo diventano fino a quando non vengono pianificate.

Nell'esempio seguente viene illustrato come creare un avviso dalla query Spazio su disco insufficiente predefinita.

1. Fare clic sulla scheda Query e rapporti, quindi sulla sottoscheda Query.

   Vengono visualizzati i riquadri Tag query ed Elenco query.
2. Fare clic sul tag Avvisi.

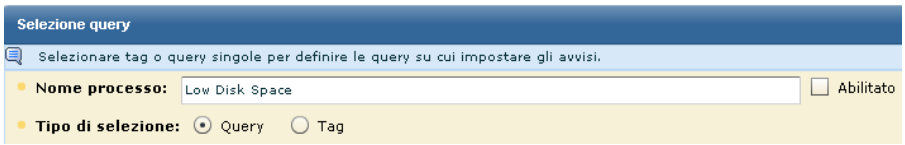
   L'Elenco query mostra le query con il tag Avvisi.
3. Fare clic sulla query Spazio su disco insufficiente nell'Elenco query.

   La query Spazio su disco insufficiente viene visualizzata nel pannello principale.

4. Fare clic su Opzioni e selezionare Pianifica avvisi.

Viene visualizzata la procedura guidata di pianificazione avvisi, con selezionato il passaggio Selezione avviso. Spazio su disco insufficiente è già selezionato in Query selezionate.

5. Specificare un nome processo, come Spazio su disco insufficiente. Per il momento, deselezionare la casella di controllo Attivato. Questo consente di salvare e chiudere la pianificazione dell'avviso prima che esso sia completo e senza rischiare un tentativo di avviarlo.



6. È possibile applicare o ignorare i filtri di avviso. I filtri sono additivi; ovvero, quando una serie di filtri viene valutata, essi vengono uniti dagli operatori logici AND.

7. Fare clic su Condizioni risultato per ignorare quelli impostati nella definizione della query.
   a. Per specificare che l'avviso deve valutare lo spazio su disco per l'ora trascorsa, inserire l'intervallo di date come "adesso" per Ora di fine dinamica e "adesso" "-1 ora" per Ora di avvio dinamica.
   b. Per specificare che si desidera ricevere una notifica soltanto se la query restituisce un risultato e per vedere soltanto il primo risultato restituito, selezionare Limite riga e inserire il valore 1. Dato che l'intervallo di tempo dinamico è espresso in ore, selezionare event_hour_datetime come Granularità tempo.
   c. Lasciare vuoto Eventi raggruppati, dal momento che non vale per questa query.

8. Fare clic su Pianifica processi per definire la pianificazione. L'impostazione predefinita prevede di iniziare il lavoro immediatamente, senza data di fine. Impostare l'intervallo di ricorrenza. Ad esempio, impostare l'intervallo in modo che la query venga eseguita ogni ora.

9. Fare clic sul passaggio Destinazione. Abilitare la notifica tramite posta elettronica. Inserire il proprio indirizzo nel campo Messaggio di posta elettronica per. (Facoltativo) Inserire un oggetto e un testo per il messaggio. Oppure, inviare il messaggio ai destinatari desiderati e inserire il proprio indirizzo di posta elettronica nel campo Da. Se si inseriscono più indirizzi, separarli con una virgola (non con un punto e virgola).

10. Fare clic su Selezione server. Per impostazione predefinita, la query verrà eseguita sul server CA User Activity Reporting Module corrente. Selezionare Federato per eseguire la query su questo server e tutte le query federate idonee.
11. Fare clic su Selezione avviso. Selezionare Attivato.
12. Fare clic su Salva e chiudi.

    Il processo di avviso viene visualizzato nella sottoscheda Pianificazione avvisi.

Processi di avviso

Nome processo	Abilitato	Server	Ricorrenza	Ora di inizio	Ora di fine	Fuso orario	Autore
Low Disk Space	true	caelm5	1 hour	Mon Sep 28 2009 10:12:08 am		America/New_York	mtest

13. Fare clic sulla scheda Gestione avvisi e su Avvisi per visualizzare i risultati di questo avviso.

Verrà ricevuta, come richiesto, la notifica tramite posta elettronica. Segue un esempio:

Oggetto: Low disk space Notification

CA Log Manager

RSS Link	https://calmrhbuildtest01:5250/spin/calm/getActionQueryResult.csp?id=J-842434629422318183 4-calmrhbuildtest011220531049152-3207977576_actionquery_1220536215721
Avviso Nome	Low Disk Space
Query Nome	Spazio su disco insufficiente
Generated Datati	10:27:11 Mer OCT 21 2009 EDT
Tags	[Action Alerts]
Autore	Administrator1
Server	calmrhbuildtest01

Commento

Disk space has dropped below 20%

Se si fa clic sul collegamento RSS, viene visualizzata una pagina simile alla seguente:

CA ELM Set di risultato di avvisi

Titolo: Spazio su disco insufficiente

Creatore: Administrator1

Fase di esecuzione: Sabato 05/12/2009 15:55:23

event_hour_datetime	receiver_hostname	dest_objectvalue

Esempio: creazione di un avviso per un evento di automonitoraggio

La query predefinita per tutti gli eventi di automonitoraggio è Dettagli relativi a tutti gli eventi di sistema. Questa query può essere copiata e utilizzata come base per definire un avviso impostato su uno specifico evento di automonitoraggio.

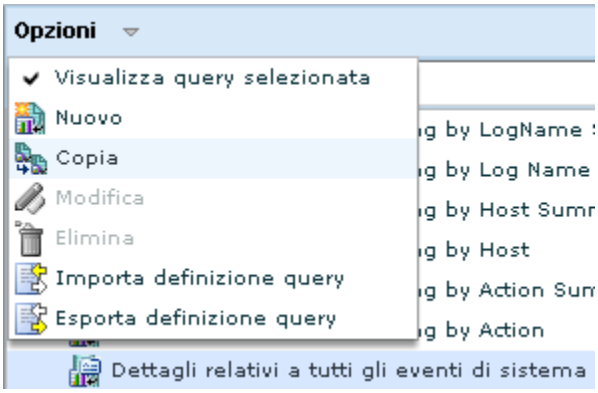
Ad esempio, si genera un evento di automonitoraggio quando un modulo che richiede di riavviare il sistema operativo viene scaricato durante un aggiornamento di sottoscrizione. Questo evento di automonitoraggio viene generato una volta sola. Si potrebbe voler creare un avviso come promemoria per il riavvio del sistema operativo, nell'eventualità che questo evento di automonitoraggio venga ignorato.

Utilizzare l'esempio seguente come guida.

1. Creare come segue una query basata sulla query per tutti gli eventi di automonitoraggio:

   a. Fare clic sulla scheda Query e rapporti, quindi sulla sottoscheda Query.

   b. Selezionare Dettagli relativi a tutti gli eventi di sistema nell'Elenco query, espandere l'elenco a discesa Opzioni e selezionare Copia.

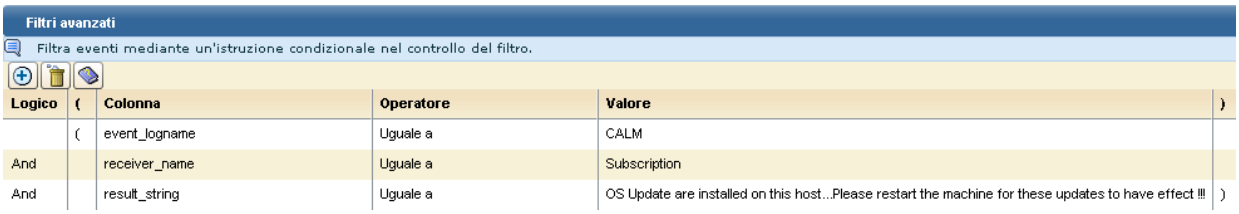


   Viene visualizzata la procedura guidata Progettazione query, con selezionato il passaggio relativo ai dettagli.

   c. Sostituire il nome della query copiata con uno nuovo, ad esempio Avviso Riavvio Sist.Op. (Facoltativo) Aggiungere un nome breve e una nuova descrizione.

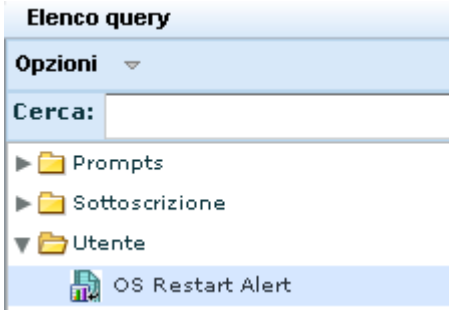
   d. Selezionare Avvisi da Tag disponibili e spostarlo in Tag selezionati.

2. Creare i filtri query nel modo seguente:
   a. Proseguire fino al passaggio Filtri query. Fare clic sulla scheda Filtri avanzati.
   b. Fare clic su Nuovo filtro evento. Selezionare event_logname per Colonna, lasciare Equal to impostato a Operatore e selezionare CALM come valore.
   c. Fare clic su Nuovo filtro evento. Selezionare receiver_name per Colonna, lasciare Equal to impostato a Operatore e immettere Sottoscrizione.
   d. Fare clic su Nuovo filtro evento. Selezionare result_string per Colonna, lasciare Equal to impostato a Operatore e immettere il messaggio Gli aggiornamenti del sistema operativo sono stati installati su questo host. Riavviare il computer perché gli aggiornamenti entrino in funzione.



3. Fare clic su Salva e chiudi.

   Il nuovo avviso verrà visualizzato nell'Elenco query sotto la cartella Utente.



4. Pianificare un avviso per la query definita dall'utente come indicato di seguito:

   a. Selezionare la query nella cartella Utente.

   b. Fare clic sul pulsante Modifica nel riquadro destro per visualizzare l'elenco a discesa Avviso Riavvio Sist.Op e selezionare Pianifica avviso.

   Viene visualizzata la procedura guidata di pianificazione avvisi, con selezionato il passaggio Selezione avviso. Avviso Riavvio Sist.Op risulta preselezionato in Query selezionate.

   c. Specificare un nome processo. Ad esempio, inserire Avviso di riavvio del sistema operativo.

5. Aggiungere un filtro evento nel modo seguente:

   a. Fare clic su Filtri di avviso.

   b. Fare clic su Nuovo filtro evento.

   c. Selezionare receiver_hostname per Colonna, lasciare Equal to impostato a Operatore e immettere il nome del CA User Activity Reporting Module locale come Valore.

6. Specificare nel modo seguente la frequenza con cui generare l'avviso quando occorre un riavvio:

   a. Fare clic su Pianifica processi.

   b. Impostare l'intervallo di ricorrenza per la frequenza di generazione dell'avviso. Ad esempio, selezionare 1 e Giorni perché la frequenza sia di una volta al giorno.

7. Fornire le proprie informazioni di posta elettronica nel modo seguente, in modo da poter essere avvisati tramite un messaggio di posta.
   a. Fare clic sul passaggio Destinazione.
   b. Fare clic su Attiva notifica tramite posta elettronica e specificare il proprio indirizzo di posta elettronica e tutte le eventuali altre informazioni desiderate.
8. Limitare come indicato di seguito la notifica alle occasioni in cui il server corrente necessita di essere riavviato:
   a. Fare clic su Selezione server.
   b. Selezionare Non per query federate.
9. Fare clic su Salva e chiudi per salvare il processo di avviso.

   Il processo di avviso appare nella scheda Gestione avvisi, sottoscheda Pianificazione avvisi.

Processi di avviso

Nome processo	Abilitato	Server	Ricorrenza	Ora di inizio	Ora di fine
Restart Operating System Alert	true	caelm5	1 day	Tue Sep 29 2009 5:13:51 pm	

Esempio: inviare un messaggio di posta elettronica all'amministratore quando si arresta il flusso degli eventi

Gli amministratori devono ricevere una notifica quando un qualsiasi connettore o agente interrompe la raccolta degli eventi. È possibile automatizzare questa notifica quando un indicatore suggerisce che si è verificata questa condizione. È possibile configurare l'indicatore, che rappresenta il tempo trascorso dal momento in cui un server di raccolta ha ricevuto eventi da un qualsiasi connettore. È possibile impostare il tempo trascorso sul numero desiderato di minuti, ore o giorni. È possibile estendere la query a tutti i server di raccolta nella federazione.

Per limitare il numero di messaggi di posta elettronica inviati quando un connettore diventa inattivo, prendere in considerazione solo quelli che hanno raccolto eventi fino ad ora. Ad esempio, impostare l'avviso in modo da restituire solo le righe dei connettori che hanno raccolto eventi nell'ora precedente, ma che non hanno raccolto eventi durante l'ultima ora.

Per acquisire questi dati, selezionare la query predefinita Connettore agente inattivo del monitor di raccolta per Gestione registro. Questa query restituisce il nome del connettore e dell'agente quando non si riceve alcun evento definito nelle condizioni di risultato dell'avviso. Utilizzare il seguente esempio come guida per generare un avviso quando, nell'ora appena trascorsa, non vengono ricevuti eventi da un connettore che ne ha inviati nel periodo compreso fra una e due ore fa. Per la destinazione dell'avviso, specificare l'indirizzo di posta elettronica della persona a cui inviare la notifica. Per la pianificazione dell'esecuzione della query, specificare una frequenza maggiore o uguale al periodo di tempo trascorso.

Nota: prima di creare l'avviso, è necessario configurare le impostazioni di posta elettronica in Amministrazione, Server di rapporto.

Per inviare un messaggio di posta elettronica all'amministratore quando un connettore interrompe la raccolta degli eventi

1. Selezionare il server da cui eseguire questo avviso. In un'architettura hub and spoke, selezionare un server di raccolta per acquisire la condizione al più presto possibile.
2. Fare clic sulla scheda Gestione avvisi e quindi sulla sottoscheda Pianificazione avvisi.
3. Fare clic su Pianifica un avviso.
4. Inserire il nome di processo, ad esempio Connettore inattivo.
5. In Query disponibili selezionare Connettore agente inattivo del monitor di raccolta per Gestione registro e spostarla nell'elenco Query selezionate.

6. Fare clic su Condizioni risultato.
7. Impostare l'orario per le ultime 2 ore.
   a. Selezionare Intervalli predefiniti: ultima ora.

      In questo modo è possibile impostare correttamente l'ora di fine dinamica su "ora", "-2 minuti"
   b. Fare clic su Modifica la stringa di tempo dinamico per Ora di inizio dinamica.
   c. In Stringa di tempo dinamico, sostituire 62 con 122.
   d. Fare clic su OK.

8. Impostare le condizioni di risultato.
   a. Selezionare Ultimi dati di evento raggruppati prima di e fare clic su Modifica
   b. Selezionare Ora per Ora di riferimento e fare clic su Aggiungi ora di riferimento alla stringa di tempo dinamico
   c. Fare clic una volta sulla casella Modifica ora per visualizzare -1, selezionare l'ora dall'elenco a discesa e fare clic su Aggiungi modifica ora alla stringa di tempo dinamico.
   d. Fare clic su OK.

9. Fare clic sul passaggio Processi pianificati e definire l'intervallo di ricorrenza. Ad esempio, impostare l'intervallo su 1 ora.

10. Fare clic su Destinazione e compilare la scheda Posta elettronica.
    a. Selezionare Attiva notifica tramite posta elettronica.
    b. Inserire l'indirizzo di posta elettronica dell'amministratore in Messaggio di posta elettronica per.
    c. Inserire il proprio indirizzo di posta elettronica in Messaggio di posta elettronica da.
    d. Immettere l'oggetto nel campo Oggetto. Ad esempio, digitare Il connettore potrebbe essere inattivo.
    e. Inserire il testo del messaggio di posta elettronica. Ad esempio digitare: la scorsa ora il connettore ha arrestato l'invio degli eventi.
11. Fare clic sul passaggio Selezione del server e, se necessario, deselezionare Federato.
12. Fare clic su Salva e chiudi.

È possibile definire questo avviso per creare una query per l'intervallo di data in giorni, anziché in ore, e quindi pianificarne l'esecuzione una volta al giorno. In questo caso, l'ora di fine dinamica verrà impostata su "ora", l'ora di avvio dinamico su "ora", "-2 giorni" e l'ultimo evento raggruppato con data anteriore verrà impostato su "ora", "-1 giorni".

Configurazione della memorizzazione degli avvisi

È possibile controllare il numero di avvisi salvati dal server di rapporto e la durata della loro memorizzazione.

Per configurare la memorizzazione degli avvisi

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.

   Viene visualizzato l'Elenco servizi.

2. Fare clic sul server di rapporto per l'impostazione globale o sull'host del server di rapporto per l'impostazione locale.

   Viene visualizzato il pannello di configurazione del server di rapporto.

3. Inserire un valore nel campo di immissione Numero massimo di avvisi. Qualsiasi avviso che superi questa soglia verrà rimosso, a partire dai meno recenti.

4. Specificare il numero dei giorni nel campo di immissione Memorizzazione avvisi; trascorso questo numero di giorni, gli avvisi vengono eliminati.

   Nota: gli avvisi vengono eliminati ogni volta che tale soglia viene superata.

5. Fare clic su Salva.

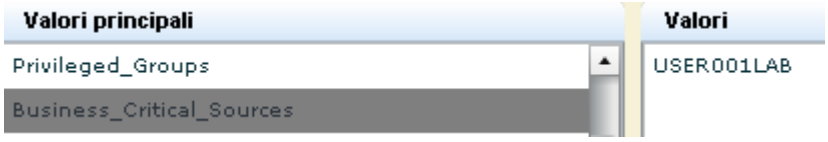
Esempio: creazione di un avviso per Business_Critical_Sources

È possibile creare una query personalizzata con l'elenco con chiave Business_Critical_Sources e pianificare un avviso basato su tale query. L'elenco con chiave non presenta valori predefiniti e nessuna query o avviso predefiniti associati. Utilizzare il seguente processo end-to-end come guida.

1. Installare un agente.

2. Configurare un connettore su quell'agente per raccogliere eventi da tutte le origini critiche di business.

3. Definire i valori del nome host per gli elenchi definiti dall'utente (chiavi) Business_Critical_Sources.
   a. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
   b. Selezionare Server di rapporto dall'Elenco server.
   c. Selezionare Business_Critical_Sources nell'area Elenchi definiti dall'utente (chiavi).
   d. Fare clic su Aggiungi valore nell'area Valori e inserire il nome host di un'origine critica di business.

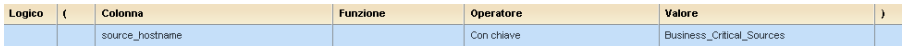


   e. Ripetere l'ultimo passaggio per ogni origine critica di business dalla quale vengono raccolti gli eventi.
   f. Fare clic su Salva.
4. Creare una query sui tentativi di accesso falliti per le origini critiche di business.
   a. Fare clic su Query e rapporti.
   b. Nell'Elenco query, immettere accesso nel campo Cerca.
   c. Selezionare Tentativi di accesso non riusciti per Host e fare clic su Copia nell'elenco a discesa Opzioni.

      Viene aperta la procedura guidata Progettazione query, con il nome Copia di Tentativi di accesso non riusciti per Host.

      Rinominare la query in Tentativi di accesso non riusciti per Business_Critical_Sources.
   d. Selezionare il passaggio Filtri query.
   e. Fare clic sulla scheda Filtri avanzati.
   f. Fare clic su Nuovo filtro evento.

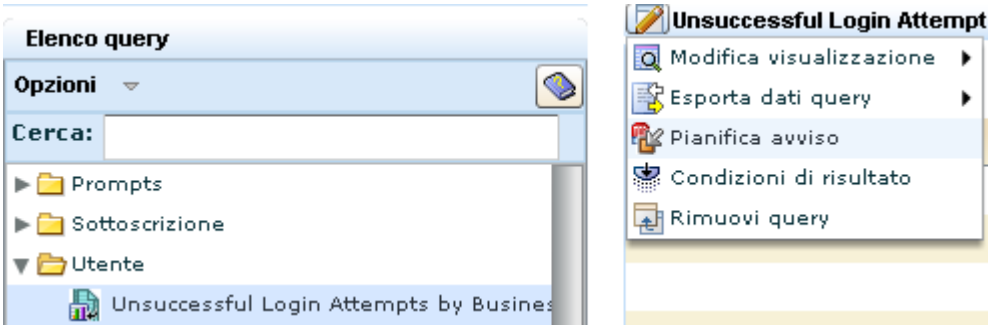
   g. Selezionare source_hostname per la colonna, Keyed come operatore e Business_Critical_Sources come valore.



Logico	(	Colonna	Funzione	Operatore	Valore	)
		source_hostname		Con chiave	Business_Critical_Sources	

   h. Fare clic su Salva e chiudi.

5. Pianificare un avviso basato su questa query personalizzata.
   a. Fare clic sulla scheda Query e rapporti.
   b. Selezionare Tentativi di accesso non riusciti per Business_Critical_Sources nella cartella Utente dell'Elenco query.
   c. Selezionare Pianifica avviso dall'elenco a discesa Modifica.



   Viene visualizzata la procedura guidata di pianificazione avvisi.
   d. Inserire un nome processo, come Tentativi di accesso non riusciti per origini critiche di business.
   e. Fare clic su Pianifica processi e definire la pianificazione.
   f. (Facoltativo) Specificare le opzioni di posta elettronica per Destinazione.
   g. Fare clic su Salva e chiudi.
6. Verificare che il processo sia stato pianificato.
   a. Fare clic sulla scheda Gestione avviso, quindi sulla sottoscheda Pianificazione avvisi.
   b. Verificare che il nome processo inserito appaia nell'elenco.

Nome processo	Abilitato	Server
Unsuccessful Login Attempts by Business Critical Resources	true	caelm8

7. Controllare che l'avviso venga generato.
   a. Fare clic sulla scheda Gestione avvisi. Viene visualizzata la sottoscheda Avvisi.
   b. Visualizzare gli avvisi elencati per determinare se il nome processo inserito compare nell'elenco.

Modifica di un avviso

È possibile modificare un avviso esistente.

Per modificare un avviso

1. Fare clic sulla scheda Gestione avvisi.

   Viene visualizzato l'elenco dei server avvisi.

2. Selezionare il server sul quale è pianificato l'avviso da modificare.

   Viene visualizzato il riquadro con i dettagli del server, che mostra per impostazione predefinita la scheda Rapporti generati.

3. Fare clic sulla scheda Avvisi pianificati, selezionare l'avviso desiderato e fare clic su Modifica in alto all'elenco.

   Viene visualizzata la procedura guidata di pianificazione avvisi.

4. Apportare le modifiche desiderate, quindi fare clic su Salva e chiudi.

   L'avviso modificato viene visualizzato nel relativo elenco.

Abilitare o disabilitare gli avvisi

È possibile disabilitare uno più avvisi quando non si desidera più eseguire le query pianificate associate a tale avviso. È possibile abilitare gli avvisi precedentemente disabilitati, in modo da eseguirli in base alla pianificazione salvata.

Per disabilitare o abilitare un processo di avviso

1. Fare clic sulla scheda Gestione avvisi e quindi sulla sottoscheda Pianificazione avvisi.

   Verrà visualizzato l'elenco Processi di avviso, la cui colonna Abilitato mostra lo stato di ogni processo. Se il processo è abilitato, il valore Abilitato sarà true. In caso contrario, il valore Abilitato sarà false.

2. Selezionare uno o più processi e fare clic su Abilita selezione o Disabilita selezione.

   Nell'elenco Processi di avviso verrà visualizzato il nuovo stato dei processi abilitati o disabilitati dall'utente.

   Nota: la possibilità di disabilitare i processi di avviso è stata concepita per l'uso con gli avvisi ricorrenti. Se si disabilita un processo di avviso con una singola occorrenza ("Una volta"), il processo verrà eliminato dall'elenco Processi di avviso.

Eliminazione di un avviso

È possibile eliminare eventuali avvisi non necessari.

Eliminazione di un avviso

1. Fare clic sulla scheda Gestione avvisi.

   Viene visualizzato l'elenco Server avvisi.

2. Selezionare il server contenente l'avviso da eliminare.

   Viene visualizzato il riquadro dei dettagli del server.

3. Fare clic sulla scheda Pianificazione rapporto, selezionare il processo desiderato facendo clic sulla riga corrispondente; quindi, fare clic su Elimina nella parte superiore dell'elenco. È possibile selezionare più processi di avviso da eliminare.

   Nota: le caselle di controllo in corrispondenza di ciascun processo di rapporto consentono l'attivazione e la disattivazione dei processi.

   Viene visualizzata una finestra di dialogo di conferma.

4. Fare clic su Sì

   Viene visualizzato un messaggio di conferma dell'eliminazione.

5. Fare clic su OK.

   Il processo di avviso viene eliminato dall'elenco Processi di avviso.

Capitolo 13: Rapporti pianificati

Questa sezione contiene i seguenti argomenti:

Visualizzazione di un rapporto generato (a pagina 497)
Annotazioni a un rapporto generato (a pagina 499)
Abilitare e disabilitare i processi di rapporto pianificati (a pagina 500)
Pianificazione di un processo di rapporto (a pagina 501)
Esempio: pianificazione di rapporti con un tag comune (a pagina 507)
Esempio: invio tramite posta elettronica di rapporti PCI in formato PDF (a pagina 511)
Modifica di un processo di rapporto pianificato (a pagina 512)
Abilitare e disabilitare i processi di rapporto pianificati (a pagina 513)
Eliminazione di un processo di rapporto pianificato (a pagina 514)
Eventi di automonitoraggio (a pagina 514)
Visualizzazione di un evento di automonitoraggio (a pagina 515)

Visualizzazione di un rapporto generato

È possibile visualizzare il rapporto generato, oppure salvarne una copia nel percorso desiderato. I rapporti generati vengono archiviati nell'applicazione software con CA User Activity Reporting Module nel percorso seguente:

```
/opt/CA/LogManager/data/reports
```

Per visualizzare un rapporto generato

1. Fare clic sulla scheda Rapporti pianificati.

   La scheda viene aperta e mostra l'host locale di CA User Activity Reporting Module per impostazione predefinita.

2. Selezionare il server su cui sono pianificati i rapporti generati che si desidera visualizzare.

   Il server selezionato viene visualizzato nel riquadro dei dettagli.

3. Fare clic sulla scheda Rapporti generati se essa non è già visualizzata.

   Viene visualizzato l'elenco Rapporti generati.

4. Fare clic sul nome del rapporto da visualizzare.

   Verrà visualizzata la finestra di dialogo Salva.

5. Fare clic su Salva per specificare una posizione in cui salvare il rapporto.

Ulteriori informazioni:

Come filtrare i rapporti (a pagina 498)
Annotazioni a un rapporto generato (a pagina 499)
Eventi di automonitoraggio (a pagina 514)

Come filtrare i rapporti

È possibile impostare filtri per perfezionare la visualizzazione dei rapporti generati e dei processi di rapporto pianificati.

Per filtrare rapporti generati o pianificati

1. Selezionare il server di rapporto in cui si trovano i rapporti pianificati o generati da filtrare e fare clic sulla scheda Rapporti generati o Rapporti pianificati.

   Viene visualizzato un elenco dei rapporti generati o pianificati.

2. Utilizzando i menu a discesa appropriati, selezionare il tipo di ricorrenza o il formato sulla base del quale filtrare i rapporti visualizzati.

   L'elenco mostrerà i rapporti che corrispondono alle qualifiche del filtro.

Ulteriori informazioni

Visualizzazione di un rapporto generato (a pagina 497)
Annotazioni a un rapporto generato (a pagina 499)

Annotazioni a un rapporto generato

È possibile aggiungere annotazioni a un rapporto generato, per scopi che includono il monitoraggio o la revisione.

Per aggiungere annotazioni a un rapporto generato

1. Selezionare il server di rapporto in cui si trovano i rapporti generati cui aggiungere annotazioni e fare clic sulla scheda Rapporti generati.

   Viene visualizzato l'Elenco rapporti.

2. Fare clic sull'icona Annotazioni accanto al rapporto interessato.

   Viene visualizzata la finestra di dialogo Annotazioni di rapporto che mostra tutte le eventuali annotazioni precedenti con il nome del creatore e l'ora e la data di creazione.

3. Inserire l'annotazione desiderata, quindi fare clic su Salva.

   L'annotazione viene visualizzata nella finestra di dialogo, che rimane aperta per consentire ulteriori annotazioni.

4. (Facoltativo) Ripetere il passaggio 3 per aggiungere ulteriori annotazioni.

5. Fare clic su Chiudi se non si ha intenzione di aggiungere altre annotazioni.

   La finestra di dialogo Annotazioni di rapporto viene chiusa.

Ulteriori informazioni

Visualizzazione di un rapporto generato (a pagina 497)
Come filtrare i rapporti (a pagina 498)

Abilitare e disabilitare i processi di rapporto pianificati

È possibile disabilitare uno o più processi di rapporto pianificati quando non si desidera più eseguire le query associati a tale rapporto. È possibile abilitare processi di rapporto pianificati precedentemente disabilitati, in modo da eseguirli in base alla pianificazione salvata.

Per disabilitare o abilitare i processi di rapporto pianificati

1. Fare clic sulla scheda Rapporti pianificati e sulla sottoscheda Pianificazione rapporto,

   Verrà visualizzato l'elenco Processi di avviso, la cui colonna Abilitato mostra lo stato di ogni processo. Se il processo è abilitato, il valore Abilitato sarà true. In caso contrario, il valore Abilitato sarà false.

2. Selezionare uno o più processi e fare clic su Abilita selezione o Disabilita selezione.

   Nell'elenco Processi pianificati verrà visualizzato il nuovo stato dei processi abilitati o disabilitati dall'utente.

   Nota: la possibilità di disabilitare i processi di rapporto nasce per l'utilizzo con i rapporti ricorrenti. Se si disabilita un processo di rapporto con una singola occorrenza ("Una volta"), il processo verrà eliminato dall'elenco Processi pianificati.

Pianificazione di un processo di rapporto

Il processo di creazione di un rapporto mediante la procedura guidata di pianificazione consiste nelle seguenti fasi principali:

1. Apertura della procedura guidata di pianificazione del rapporto.
2. Selezione dei modelli di rapporto: per iniziare la pianificazione di un processo di rapporto, è necessario selezionare il rapporto o tag che si desidera utilizzare come modello. È possibile selezionare tag e modelli singoli o multipli.

   Nota: è possibile pianificare un rapporto indirizzato verso un database ODBC esterno. Per eseguire l'operazione, configurare le connessioni verso i database ODBC selezionati, quindi creare query e rapporti indirizzati verso tali database. L'installazione non fornisce query o report ODBC.
3. Creazione di filtri di rapporto: è possibile applicare filtri di rapporto avanzati per personalizzare ulteriormente i risultati del rapporto in base alle proprie esigenze.
4. Impostazione dell'intervallo di date e delle condizioni di risultato - È possibile definire l'intervallo di date per l'esecuzione di ricerche e altre condizioni.
5. Pianificazione di processi - Impostare la data e l'ora di esecuzione dei rapporti a ricorrenza singola o a ricorrenza multipla. È inoltre possibile selezionare i modelli ricorrenti disponibili.
6. Selezione di un formato di rapporto e di una destinazione - È possibile selezionare il formato di rapporto desiderato e le opzioni di consegna di posta elettronica.
7. Selezione di un server - Selezionare il server interrogato dal rapporto e specificare se la query viene estesa a un altro host federato. Si tratta di un'operazione non richiesta per i rapporti ODBC esterni.

Apertura della procedura guidata Pianificazione rapporto

Per creare un nuovo processo di rapporto per uno o più rapporti ricorrenti, è necessario utilizzare la procedura guidata Pianificazione rapporto.

Per aprire la procedura guidata Pianificazione rapporto

1. Fare clic sulla scheda Rapporti pianificati.

   Viene visualizzato l'elenco dei server di rapporto.

2. Selezionare il server sul quale si desidera pianificare il rapporto.

   Il pannello Dettagli server rapporti mostra il server selezionato e, per impostazione predefinita, la scheda Rapporti generati.

3. Fare clic sulla scheda Pianificazione rapporto, quindi su Pianifica un rapporto.

   Viene visualizzata la procedura guidata Pianificazione rapporto.

   Mentre si utilizza la procedura guidata:

   - Fare clic su Salva e chiudi per salvare il rapporto pianificato e chiudere la procedura.
   - Fare clic su Ripristina per ripristinare la visualizzazione della procedura alle ultime impostazioni salvate.

Ulteriori informazioni

Impostazione dei parametri di pianificazione (a pagina 505)
Creazione di un filtro di eventi avanzato (a pagina 586)
Scelta della destinazione delle query di un rapporto (a pagina 507)

Selezione di un modello di rapporto

Il primo passo verso la creazione di un processo di rapporto è la selezione del modello di rapporto. Per pianificare più processi di rapporto che condividono gli stessi filtri, la stessa pianificazione e le stesse impostazioni di destinazione, selezionare più rapporti o tag come modelli.

Se si selezionano più rapporti, i processi verranno visualizzati separatamente per ogni rapporto. Ad esempio, se si selezionano due rapporti differenti, tali rapporti condivideranno le stesse opzioni di pianificazione e di applicazione del filtro, ma verranno visualizzati separatamente e intitolati in base al nome del rapporto nell'elenco Rapporti generati.

Gli utenti con il ruolo di Amministratore possono creare processi di rapporto con stato disabilitato per l'utilizzo futuro. Gli utenti con ruoli di Administrator e Analyst possono abilitare e disabilitare i processi in un secondo momento. I rapporti disabilitati visualizzano il valore *false* nella colonna Disabilitato quando si visualizza la scheda Rapporti pianificati.

Per selezionare un modello di rapporto

1. Immettere un nome del processo.
2. Selezionare il fuso orario in cui si desidera pianificare il rapporto dal menu a discesa dei fusi orari.
3. Selezionare la destinazione del rapporto pianificato mediante l'elenco a discesa Connessione. Il valore UARM predefinito viene visualizzato nell'elenco a discesa assieme ai nomi delle connessioni ODBC impostate nell'area Servizio di rapporto.

   UARM predefinito

   Indirizza il rapporto ai database di eventi interni e di incidenti.

   Connessioni ODBC

   Indirizza il rapporto a una tabella ODBC esterna selezionata. Verrà visualizzato l'elenco a discesa Tabella contenente le tabelle disponibili per il database selezionato.
4. Se si seleziona una connessione ODBC, selezionare la tabella desiderata dall'elenco a discesa Tabella.
5. Selezionare il pulsante Rapporti o Tag per selezionare i rapporti in base al tag o individualmente.

Nota: la pianificazione dei rapporti per tag consente di aggiungere rapporti senza alterare il processo stesso. Se si seleziona il tag Gestione identità, qualsiasi rapporto con tale tag viene aggiunto al processo all'ora di avvio pianificata. Questa caratteristica si applica anche ai tag personalizzati.

6. (Facoltativo) Selezionare un tag o più tag per restringere il numero di tag e rapporti individuali selezionati. Questa caratteristica corrisponde al comportamento dell'Elenco rapporti.
7. (Facoltativo) Deselezionare la casella di controllo Attiva per creare il processo di rapporto in stato disabilitato. La casella di controllo Attiva è selezionata per impostazione predefinita.

   Nota: la possibilità di creare un processo di rapporto disabilitato è progettata per l'uso con i rapporti ricorrenti. Se si crea un processo disattivato con una singola occorrenza (Adesso o Una volta), tale processo verrà rimosso dall'elenco dei rapporti pianificati.
8. (Facoltativo) Selezionare la casella di controllo Mantieni dopo la scadenza per conservare la configurazione del rapporto dopo la generazione del rapporto.

   Nota: dopo aver generato il rapporto, è possibile modificare il modello di rapporto e pianificare nuovamente il rapporto.
9. Selezionare i tag o i rapporti che si desidera utilizzare come modelli di rapporto. Quindi utilizzare il controllo pilota per aggiungerli all'area Rapporti selezionati.
10. Procedere con il passaggio di pianificazione che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

    Facendo clic su Salva e chiudi, il rapporto viene pianificato; altrimenti, verrà visualizzato il passaggio selezionato.

Impostazione dei parametri di pianificazione

È possibile controllare l'avvio dei rapporti pianificati, se si desidera impostarli come rapporti ricorrenti e il relativo intervallo di ricorrenza.

Per impostare i parametri di pianificazione

1. Avviare la procedura guidata Pianificazione rapporto e andare al passaggio Pianifica processi.
2. Utilizzare i pulsanti di opzione Non ricorrente o Ricorrente per selezionare l'ora della generazione del rapporto e il tipo di ricorrenza desiderato, se impostato.

   Nota: se nel proprio ambiente viene utilizzata l'ora legale, non pianificare rapporti durante il cambiamento d'ora, altrimenti tali rapporti non verranno generati. Ad esempio, se l'ora legale inizia alle 2.00 dell'8 marzo, non sarà possibile generare un rapporto tra le 2.00.00 e le 2.59.59.
3. Procedere con il passaggio di pianificazione che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, il rapporto viene pianificato; altrimenti, verrà visualizzato il passaggio selezionato.

Ulteriori informazioni

Utilizzo di filtri avanzati (a pagina 584)
Scelta della destinazione delle query di un rapporto (a pagina 507)

Selezione delle impostazioni relative a formato e notifiche

È possibile scegliere se generare i rapporti in formato PDF, Excel o XML. Si può anche impostare una notifica automatica tramite posta elettronica.

Per impostare il formato e la notifica

1. Avviare la procedura guidata Pianificazione rapporto e andare al passaggio Destinazione.
2. Scegliere il formato desiderato dal menu a discesa Formato rapporto.

   Nota: nel formato PDF, i grafici sono limitati a 100 punti dati, il che mantiene le etichette degli assi del grafico chiaramente leggibili. Se il grafico che si desidera visualizzare contiene più di 100 punti, CA User Activity Reporting Module include solo i primi 100 nell'output PDF pubblicato.
3. Selezionare la casella di controllo Posta elettronica se si desidera inviare una notifica quando viene generato un rapporto.

   Verranno visualizzati i campi di specifica della posta elettronica.
4. Inserire gli indirizzi di posta elettronica di tutti gli utenti cui si desidera inviare la notifica. Separare gli indirizzi multipli con le virgole.
5. (Facoltativo) Inserire le altre specifiche desiderate, compreso l'oggetto, l'indirizzo di posta elettronica cui inviare la risposta e il corpo del testo.
6. (Facoltativo) Selezionare Allega rapporto per allegare una copia del rapporto nel formato scelto al messaggio e-mail di notifica.
7. Procedere con il passaggio di pianificazione che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Facendo clic su Salva e chiudi, il rapporto viene pianificato; altrimenti, verrà visualizzato il passaggio selezionato.

Ulteriori informazioni:

Utilizzo di filtri avanzati (a pagina 584)
Impostazione dei parametri di pianificazione (a pagina 505)
Scelta della destinazione delle query di un rapporto (a pagina 507)

Scelta della destinazione delle query di un rapporto

È possibile scegliere in quale archivio registro eventi federato verrà eseguita la ricerca da parte della query del rapporto.

Per scegliere le destinazioni del rapporto

1. Avviare la procedura guidata Pianificazione rapporto e andare al passaggio Selezione server.
2. Selezionare gli eventuali server disponibili cui si vuole indirizzare la query e trasferirli nell'area Server selezionati utilizzando il controllo pilota.
3. (Facoltativo) Per disabilitare le query federate per questo rapporto, selezionare "No" dal menu a discesa che appare quando si fa clic sulla voce Query federate. Le query dei rapporti sono federate per impostazione predefinita.
4. Procedere con il passaggio di pianificazione che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, il rapporto viene pianificato; altrimenti, verrà visualizzato il passaggio selezionato.

Ulteriori informazioni

Utilizzo di filtri avanzati (a pagina 584)
Impostazione dei parametri di pianificazione (a pagina 505)

Esempio: pianificazione di rapporti con un tag comune

È possibile pianificare uno o più rapporti che devono essere generati con la frequenza specificata con la data di fine specificata.

Revisori, analisti e amministratori possono pianificare i rapporti.

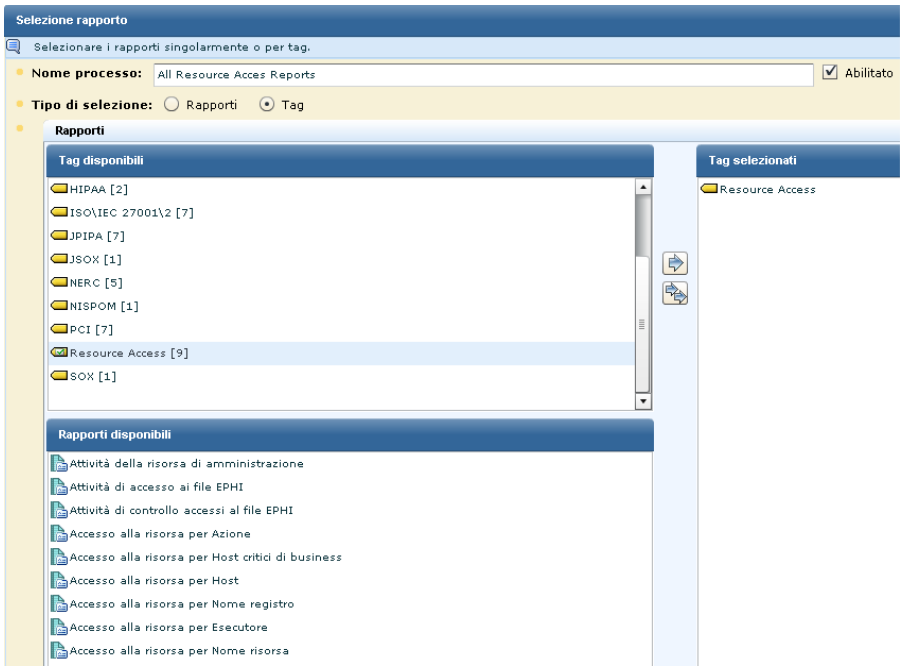
Per pianificare un rapporto

1. Fare clic sulla scheda Rapporti pianificati, quindi sulla sottoscheda Pianificazione rapporto e infine su Pianifica un rapporto.

Viene visualizzata la procedura guidata Pianificazione rapporto, che mostra il passaggio 1, Selezione rapporto.

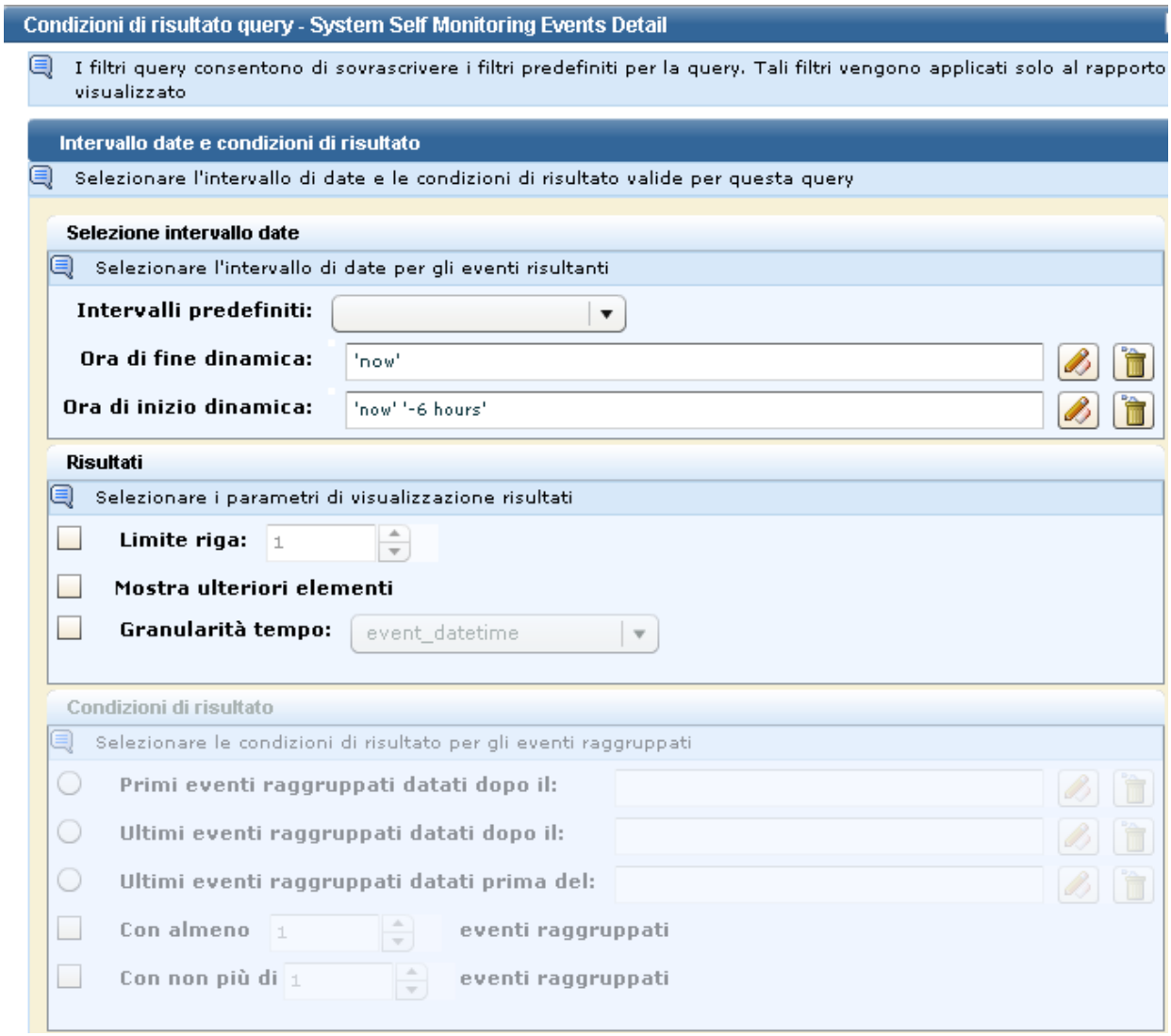
2. Inserire un nome per il processo, selezionare Rapporti per abilitare la selezione di rapporti individuali o selezionare Tag per abilitare la selezione di tutti i rapporti associati a un tag selezionato.

   Nell'esempio seguente, la selezione dei tag di accesso alla risorsa è un metodo semplice per selezionare i sei rapporti con questo tag.



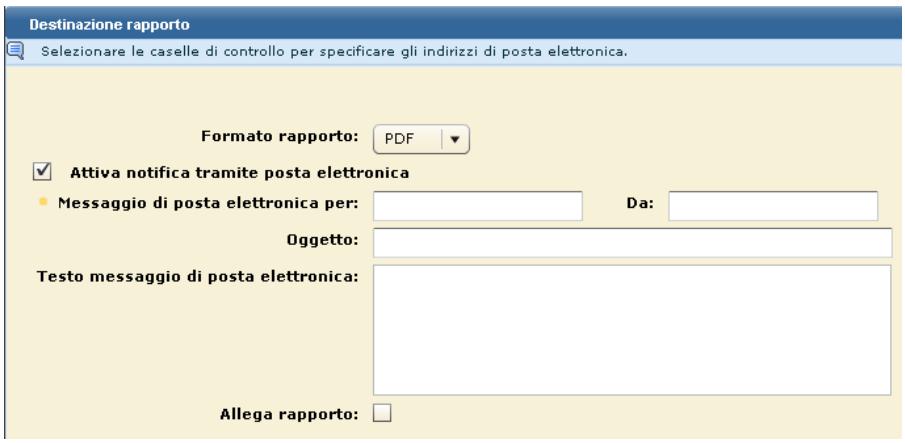
3. (Facoltativo) Fare clic su Filtri di rapporto e creare un nuovo filtro evento per limitare il rapporto ai dati necessari.

4. (Facoltativo) Fare clic su Condizioni risultato e selezionare un intervallo di date e/o le condizioni risultato per questa query. Ad esempio, per cercare eventi verificatisi nell'arco delle ultime sei ore, selezionare "ora" come ora di fine dinamica e selezionare "ora" e "-6 ore" come ora di inizio dinamica. Selezionare Limite riga e scegliere un numero, ad esempio 250.



5. Fare clic su Processi pianificati per pianificare la generazione su Ora o selezionare un'altra opzione e specificare i dettagli.

6. Fare clic su Destinazione, specificare se formattare il rapporto come foglio di calcolo di Excel, PDF o XML. Il foglio di calcolo è adatto ai dati tabulari, il PDF per i grafici. Facoltativamente, si può inviare una notifica tramite posta elettronica (utilizzare la virgola per delimitare gli indirizzi di posta). Il messaggio può essere inviato senza rapporto, come semplice conferma della generazione del rapporto pianificato; altrimenti, è possibile inviarlo come allegato.



Nota: l'amministratore può configurare i rapporti perché vengano eliminati dopo un periodo di memorizzazione specificato. Conservare una copia del messaggio può servire come alternativa di backup all'archiviazione manuale.

7. Fare clic su Selezione server e selezionare uno o più server per i rapporti e indicare se inviare una query alla federazione di server.

8. Fare clic su Salva e chiudi.

   I rapporti selezionati vengono pianificati per la generazione.

Processi pianificati

Nome processo	Server	Tipo	Ora pianificata	Autore
All Resource Access Reports	caelm5	tags	Mon Sep 28 2009 2:33:57 am	admin

Esempio: invio tramite posta elettronica di rapporti PCI in formato PDF

È possibile automatizzare il recapito di rapporti specifici nel formato scelto, alla persona specificata e secondo la frequenza richiesta.

Prima di poter specificare che i rapporti pianificati siano formattati come PDF e allegati ai messaggi di posta elettronica, è necessario configurare quanto segue in Configurazione globale per Server di rapporto nella scheda Amministrazione e nella sottoscheda Servizi.

- Opzioni del server di posta elettronica:
  - Server posta elettronica
  - Porta SMTP (25)
  - Messaggio di posta elettronica di amministrazione
  - Nome utente e password SMTP
- Specifiche del PDF:
  - Nome azienda/prodotto
  - URL logo azienda/prodotto
  - Carattere di intestazione e dimensioni del carattere
  - Carattere dei dati e dimensioni del carattere
  - Orientamento, larghezza e altezza della pagina

Esempio: recapito di tutti i rapporti PCI giornalieri in formato PDF alla casella di posta in arrivo del revisore tutti i giorni della settimana

1. Fare clic sulla scheda Rapporti pianificati, quindi sulla sottoscheda Pianificazione rapporto.

   Sulla barra degli strumenti viene visualizzato il pulsante Pianificazione rapporto.

2. Fare clic su Pianifica rapporto.

   Viene visualizzato il passaggio Selezione rapporti.

3. Selezionare un rapporto nel modo seguente:
   a. Inserire Rapporti PCI come nome del processo.
   b. Selezionare Tag come tipo di selezione.
   c. Selezionare PCI da Tag disponibili e spostarlo in Tag selezionati.

4. Pianificare il processo nel modo seguente:
   a. Fare clic sul passaggio Pianifica processi.
   b. Selezionare Giornaliero come ricorrenza.
   c. Selezionare tutti i giorni della settimana.
5. Specificare la destinazione del rapporto e il formato nel modo seguente:
   a. Fare clic sulla scheda Destinazione.
   b. Accettare il formato predefinito del rapporto, ovvero il formato PDF.
   c. Selezionare Attiva notifica tramite posta elettronica.
   d. Inserire l'indirizzo di posta elettronica del revisore. Utilizzare la sintassi seguente: <nome_email>@<azienda>.com
   e. Selezionare Allega rapporto.
6. Fare clic su Salva e chiudi.

Modifica di un processo di rapporto pianificato

È possibile modificare un processo di rapporto pianificato.

Per modificare un processo di rapporto pianificato

1. Fare clic sulla scheda Rapporti pianificati.

   Verrà visualizzato l'elenco dei server di rapporto.
2. Selezionare il server sul quale è pianificato il rapporto da modificare.

   Il server selezionato viene visualizzato nel pannello Dettagli server rapporti.
3. Selezionare il processo di rapporto desiderato, quindi fare clic su Modifica nella parte superiore dell'elenco.

   Viene visualizzata la procedura guidata Pianificazione rapporto.
4. Apportare le modifiche desiderate e fare clic su Salva e chiudi.

   Il rapporto modificato viene visualizzato nell'elenco dei processi pianificati entro 5 minuti, non appena viene eseguito l'aggiornamento dell'elenco. Fare clic su Aggiorna per poterlo visualizzare immediatamente.

Ulteriori informazioni:

Eliminazione di un processo di rapporto pianificato (a pagina 514)

Abilitare e disabilitare i processi di rapporto pianificati

È possibile disabilitare uno o più processi di rapporto pianificati quando non si desidera più eseguire le query associati a tale rapporto. È possibile abilitare processi di rapporto pianificati precedentemente disabilitati, in modo da eseguirli in base alla pianificazione salvata.

Per disabilitare o abilitare i processi di rapporto pianificati

1. Fare clic sulla scheda Rapporti pianificati e sulla sottoscheda Pianificazione rapporto,

   Verrà visualizzato l'elenco Processi di avviso, la cui colonna Abilitato mostra lo stato di ogni processo. Se il processo è abilitato, il valore Abilitato sarà true. In caso contrario, il valore Abilitato sarà false.

2. Selezionare uno o più processi e fare clic su Abilita selezione o Disabilita selezione.

   Nell'elenco Processi pianificati verrà visualizzato il nuovo stato dei processi abilitati o disabilitati dall'utente.

   Nota: la possibilità di disabilitare i processi di rapporto nasce per l'utilizzo con i rapporti ricorrenti. Se si disabilita un processo di rapporto con una singola occorrenza ("Una volta"), il processo verrà eliminato dall'elenco Processi pianificati.

Eliminazione di un processo di rapporto pianificato

È possibile eliminare un processo di rapporto pianificato.

Per eliminare un processo di rapporto pianificato

1. Fare clic sulla scheda Rapporti pianificati.

   Verrà visualizzato l'elenco dei server di rapporto.

2. Selezionare il server sul quale è pianificato il rapporto da eliminare.

   Il server selezionato viene visualizzato nel pannello Dettagli server rapporti.

3. Fare clic sulla scheda Pianificazione rapporto, selezionare il processo desiderato facendo clic sulla riga corrispondente; quindi, fare clic su Elimina nella parte superiore dell'elenco. È possibile selezionare più processi da eliminare.

   Nota: le caselle di controllo in corrispondenza di ciascun processo di rapporto consentono l'attivazione e la disattivazione dei processi.

   Viene visualizzata una finestra di dialogo di conferma.

4. Fare clic su Sì

   Il processo di rapporto viene rimosso dall'elenco Processi pianificati.

Ulteriori informazioni:

Modifica di un processo di rapporto pianificato (a pagina 512)

Eventi di automonitoraggio

La maggior parte delle azioni compiute dall'utente genera eventi di automonitoraggio che consentono di tenere traccia delle azioni eseguite o che hanno coinvolto il server e del relativo esito positivo o negativo. Gli eventi di automonitoraggio vengono visualizzati nel formato Visualizzatore eventi per ogni server nelle schede Rapporti pianificati e Gestione avvisi. È anche possibile accedere a essi come rapporti normali o pianificati tramite il rapporto Eventi di automonitoraggio.

Ulteriori informazioni

Visualizzazione di un evento di automonitoraggio (a pagina 515)

Visualizzazione di un evento di automonitoraggio

Dalle schede Gestione avvisi e Rapporti pianificati è possibile visualizzare eventi di automonitoraggio relativi a ogni server. Ciò che mostra ogni scheda viene filtrato in modo da visualizzare tutti gli eventi rilevanti di monitoraggio di avvisi o rapporti. È possibile rimuovere il filtro e visualizzare tutti gli eventi di automonitoraggio.

Per visualizzare eventi di automonitoraggio

1. Fare clic sulla scheda Rapporti pianificati o Gestione avvisi.

   Viene visualizzato l'elenco dei server di rapporto o di avviso.

2. Selezionare il server di cui si desidera visualizzare gli eventi di automonitoraggio.

   Il server selezionato viene visualizzato nel riquadro dei dettagli.

3. Fare clic sulla scheda Eventi di automonitoraggio.

   Appare il pannello Visualizzatore eventi di automonitoraggio, che mostra gli eventi di automonitoraggio relativi a report o avvisi in cui è possibile eseguire le comuni attività relative ai rapporti, tra cui:

   - Attività di visualizzatore eventi
   - Filtraggio globale o locale
   - Impostazione dei Preferiti
   - Esportazione

Capitolo 14: Soppressione e riepilogo

Questa sezione contiene i seguenti argomenti:

Versioni dei componenti per il perfezionamento degli eventi (a pagina 517)
Attività relative alle regole per la soppressione e il riepilogo (a pagina 518)
Creazione di una regola di soppressione per l'evento Windows 560 (a pagina 542)

Versioni dei componenti per il perfezionamento degli eventi

CA User Activity Reporting Module memorizza le versioni precedenti di alcuni componenti personalizzati di perfezionamento eventi mentre essi vengono creati e modificati. Questo consente di fare riferimento alle versioni precedenti. È possibile visualizzare o copiare versioni dei componenti seguenti:

- File di analisi del messaggio
- File di mapping dei dati
- Regole di soppressione
- Regole di riepilogo

Ogni volta che viene creato un nuovo componente personalizzato, viene designato come Versione 1.0. Quando si modifica e si salva una nuova versione dello stesso oggetto, viene designata come Versione 2.0. Entrambe le versioni vengono visualizzate nell'area appropriata dell'interfaccia per la selezione e l'applicazione.

Ad esempio, se viene creata una regola di soppressione personalizzata chiamata "NuovaRegola", essa viene visualizzata come NuovaRegola Versione 1.0 nell'elenco dell'interfaccia Archivio registro eventi per l'applicazione. Se il file viene successivamente modificato, viene visualizzato come NuovaRegola Versione 2.0 nell'elenco Archivio registro eventi.

È possibile visualizzare le versioni precedenti dei componenti di perfezionamento eventi nell'elenco appropriato. Sono di sola lettura e non possono essere modificate. È possibile copiare una versione precedente e modificarla, rendendola a sua volta una nuova versione. Quindi, tornando all'esempio, non è possibile modificare NuovaRegola Versione 1.0 se esiste una Versione 2.0. Sarà necessario copiare la Versione 1.0 e modificarla. Il salvataggio delle modifiche creerà la Versione 3.0.

Ulteriori informazioni

Modifica di una regola per la soppressione o il riepilogo (a pagina 538)

Attività relative alle regole per la soppressione e il riepilogo

Le regole per la soppressione e il riepilogo consentono di controllare il flusso degli eventi e di gestire la dimensione degli archivi registro eventi eliminando o combinando alcuni eventi. Le regole di soppressione impediscono completamente la registrazione degli eventi nativi che corrispondono alle loro qualificazioni. Le regole di riepilogo combinano più eventi nativi in un unico evento perfezionato, che appare al posto degli eventi del componente originale.

Importante: le regole di soppressione e riepilogo dovrebbero essere utilizzate con cautela, dal momento che possono impedire la registrazione e l'apparizione di alcuni eventi nativi. È consigliabile verificare le regole personalizzate di soppressione e riepilogo in un ambiente di prova prima di distribuirle.

Le attività di soppressione e riepilogo possono essere tutte eseguite dall'area Raccolta registri dell'interfaccia. È possibile creare, modificare ed eliminare le regole di soppressione e riepilogo personalizzate.

Ulteriori informazioni

Modalità di creazione di una regola per la soppressione (a pagina 520)
Modalità di creazione di una regola per il riepilogo (a pagina 526)
Applicazione di una regola di soppressione o riepilogo (a pagina 533)
Copia di una regola di soppressione o riepilogo (a pagina 537)
Modifica di una regola per la soppressione o il riepilogo (a pagina 538)
Eliminazione di una regola per la soppressione o il riepilogo (a pagina 539)
Importazione di una regola per la soppressione o il riepilogo (a pagina 540)
Esportazione di una regola per la soppressione o il riepilogo (a pagina 541)

Effetti della regola di soppressione

Durante la pianificazione, è consigliabile riflettere sugli effetti delle *regole di soppressione*, che impediscono agli eventi di essere inseriti nell'archivio registro eventi o di essere raccolti da un connettore. Le regole di soppressione sono sempre collegate a un connettore. È possibile applicare regole di soppressione a livello di agente o gruppo, oppure al server CA User Activity Reporting Module stesso. Gli effetti differiscono in base alla posizione:

- Le regole di soppressione applicate a livello dell'agente o del gruppo impediscono agli eventi di essere raccolti, riducendo quindi l'importo del traffico di rete *inviato* al server CA User Activity Reporting Module.
- Le regole di soppressione applicate al server CA User Activity Reporting Module impediscono agli eventi di essere *inseriti* nel database, riducendo quindi la quantità di informazioni archiviate.

Occorre fare delle considerazioni sulle prestazioni potenziali derivanti dall'applicazione delle regole di soppressione agli eventi dopo il loro arrivo sul server CA User Activity Reporting Module, in particolare se si creano più regole di soppressione o se la velocità del flusso degli eventi è elevata.

Ad esempio, è consigliabile eliminare *alcuni* eventi da un firewall o da alcuni server Windows che producono eventi duplicati per la stessa azione. La mancata raccolta di questi eventi può velocizzare il trasferimento dei registri evento che si desidera mantenere e far risparmiare tempo per l'elaborazione sul server CA User Activity Reporting Module. In casi simili, applicare una o più regole di soppressione adeguate ai componenti degli agenti.

Se si desidera eliminare tutti gli eventi di un certo tipo da più piattaforme o nell'intero ambiente, applicare una o più regole di soppressione adeguate sul server CA User Activity Reporting Module. La valutazione degli eventi in merito alla soppressione si verifica quando gli eventi arrivano al server CA User Activity Reporting Module. L'applicazione di un vasto numero di regole di soppressione al server può portare a un rallentamento delle prestazioni, poiché il server deve applicare le regole di soppressione oltre a inserire gli eventi nell'archivio registro eventi.

Per le implementazioni più piccole, la soppressione può essere eseguita sul server CA User Activity Reporting Module. Si può anche scegliere di applicare la soppressione sul server per le distribuzioni in cui è in uso il riepilogo (aggregazione). Se si stanno inserendo soltanto alcuni degli eventi da un'origine che genera grandi quantità di informazioni, si può sempre scegliere di eliminare gli eventi indesiderati a livello di agente o di gruppo di agenti per risparmiare tempo per l'elaborazione sul server CA User Activity Reporting Module.

Modalità di creazione di una regola per la soppressione

È possibile utilizzare regole di soppressione per evitare che grandi quantità di transazioni di routine o note e prevedibili ingombrino l'archivio registro eventi e rendano confusa l'immagine dell'ambiente. Ad esempio, si può usare una regola per la soppressione per eliminare eventi di informazioni syslog non necessari, in particolare in casi in cui non è possibile configurare l'origine evento per trasmettere soltanto il set richiesto.

La creazione di una regola per la soppressione tramite la relativa procedura guidata si articola nei passaggi seguenti:

1. Apertura della procedura guidata regola di soppressione.
2. Denominazione della regola: specifica di un nome per la regola e informazioni descrittive.
3. Selezione evento: identificazione di un evento di cui eseguire la soppressione tramite gli attributi di normalizzazione CEG e i filtri avanzati facoltativi.

Nota: una volta creata una regola per la soppressione, occorre applicarla perché sia utilizzabile nel proprio ambiente.

Ulteriori informazioni

Apertura della procedura guidata di soppressione (a pagina 521)
Denominazione di una regola di soppressione (a pagina 521)
Applicazione di una regola di soppressione o riepilogo (a pagina 533)

Apertura della procedura guidata di soppressione

Per creare una nuova regola di soppressione o modificarne una esistente, aprire la procedura guidata di soppressione.

Per aprire la procedura guidata di soppressione

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Raccolta registri.

   Viene visualizzato l'elenco della cartella Raccolta registri.

2. Fare clic sulla freccia accanto alla cartella Libreria di perfezionamento eventi per espanderla; quindi, selezionare la cartella Soppressione e riepilogo.

   Nel riquadro dei dettagli vengono visualizzati i pulsanti per la soppressione e il riepilogo.

3. Fare clic su Nuova regola di soppressione:

   Viene visualizzata la procedura guidata di soppressione.

   Mentre si utilizza la procedura guidata:

   - Fare clic su Salva per salvare il file della regola senza chiudere la procedura.
   - Fare clic su Salva e chiudi per salvare il file della regola e chiudere la procedura.
   - Fare clic su Ripristina per ripristinare la visualizzazione della procedura alle ultime impostazioni salvate.

Ulteriori informazioni

Denominazione di una regola di soppressione (a pagina 521)

Denominazione di una regola di soppressione

È necessario denominare le regole di soppressione. È inoltre possibile immettere informazioni descrittive facoltative di riferimento.

Per denominare una regola di soppressione

1. Aprire la procedura guidata di soppressione.
2. Specificare un nome per la nuova regola.
3. (Facoltativo) Digitare informazioni descrittive.
4. Proseguire con il passaggio Filtraggio.

Ulteriori informazioni

Modalità di creazione di una regola per la soppressione (a pagina 520)

Selezione di un evento di cui eseguire la soppressione

È necessario specificare l'evento nativo di cui eseguire la soppressione impostando un filtro semplice per i campi di normalizzazione degli eventi CEG. Questi quattro campi, che fanno parte della classe specifica di eventi, vengono forniti per tutti gli eventi espressi in CEG e consentono di identificare con precisione un evento nativo.

È possibile specificare la combinazione di campi di normalizzazione degli eventi che si desidera utilizzare nella scheda Filtri semplici. È possibile utilizzare i filtri avanzati per ulteriori dettagli nell'identificazione degli eventi. È necessario specificare almeno un filtro semplice per una regola di soppressione.

Per selezionare un evento regola di soppressione

1. Aprire la procedura guidata di soppressione, inserire le informazioni richieste e andare al passaggio Filtraggio.
2. Per creare filtri semplici che consentano di selezionare l'evento desiderato, selezionare la casella di controllo appropriata, quindi selezionare o immettere il valore desiderato. Di seguito sono elencati i campi disponibili:

   Modello ideale

   In questo campo viene descritta la categoria tecnologica generica inclusa nell'evento, ad esempio Firewall o Periferica di rete.

   Categoria evento

   In questo campo vengono descritte le categorie generali di eventi all'interno del campo Modello ideale. Ad esempio tutti gli eventi relativi agli account, ai gruppi di utenti e ai ruoli sono inclusi nella categoria di evento "Gestione identità". Ogni categoria di evento dispone di una o più classi (categorie secondarie), quindi le opzioni disponibili nel menu Classe evento variano a seconda della selezione effettuata.

   Classe evento

   Consente una classificazione più dettagliata degli eventi di una categoria specifica. Ad esempio, gli eventi Gestione identità sono divisi in una delle tre classi: account, gruppo o identità. A ogni categoria di evento sono associate una o più azioni, quindi le opzioni disponibili nel menu Azione evento variano a seconda della selezione effettuata.

Azione evento

Descrive azioni comuni per ogni categoria e classe di eventi. Ad esempio, Gestione account, una classe della categoria Gestione identità, contiene le azioni di creazione, eliminazione e modifica dell'account.

3. Fare clic sulla freccia appropriata per andare al passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, la nuova regola verrà visualizzata nell'elenco. In alternativa, apparirà il passaggio scelto della procedura guidata.

Quando viene creata una nuova regola, essa viene salvata come versione 1.0. Se in seguito la regola viene modificata, una copia separata di essa viene memorizzata come nuova versione. È possibile visualizzare le versioni precedenti e applicarle o copiarle, secondo necessità.

Ulteriori informazioni:

Creazione di un filtro evento semplice (a pagina 584)
Creazione di un filtro di eventi avanzato (a pagina 586)
Utilizzo di filtri avanzati (a pagina 524)

Utilizzo di filtri avanzati

È possibile utilizzare filtri avanzati per qualificare tutte le query relative alla soppressione o al riepilogo del deposito eventi di log. L'interfaccia Filtri avanzati consente di creare la sintassi appropriata dei filtri mediante un modulo in cui è possibile immettere termini logici, colonne, operatori e valori in base ai requisiti delle regole di soppressione o riepilogo.

Nota: nella presente sezione è contenuta una breve panoramica dei termini utilizzati nei filtri avanzati per le regole di soppressione e di riepilogo. Per sfruttare al massimo i filtri avanzati, occorre una conoscenza approfondita della terminologia dei filtri e della Grammatica evento comune (CEG).

I termini elencati di seguito vengono usati per unire più istruzioni di filtro:

And

Consente di visualizzare le informazioni sugli eventi se *tutti* i termini associati risultano veri.

Oppure

Consente di visualizzare le informazioni sugli eventi se *uno* dei termini associati risulta vero.

I seguenti operatori SQL vengono utilizzati dai filtri avanzati per creare le condizioni di base per la soppressione o il riepilogo:

Corrispondenza

Include tutte le informazioni evento che corrispondono a uno o più caratteri della stringa alfanumerica immessa, consentendo di eseguire una ricerca per parole chiave. Questa ricerca rileva la distinzione tra maiuscole e minuscole.

Corrispondenza (Ignora maiuscole/minuscole)

Include tutte le informazioni evento che corrispondono a uno o più caratteri della stringa alfanumerica immessa, consentendo di eseguire una ricerca per parole chiave. Questa ricerca non rileva la distinzione tra maiuscole e minuscole.

Corrispondenza non trovata

Include le informazioni sugli eventi che non corrispondono a uno o più caratteri della stringa alfanumerica immessa. Questa ricerca rileva la distinzione tra maiuscole e minuscole.

Corrispondenza non trovata (Ignora maiuscole/minuscole)

Include le informazioni sugli eventi che non corrispondono a uno o più caratteri della stringa alfanumerica immessa. Questa ricerca non rileva la distinzione tra maiuscole e minuscole.

Corrispondenza con espressione regolare

Include le informazioni sugli eventi che corrispondono a uno o più dei caratteri di espressione regolare immessi. Questa opzione può essere utilizzata per le ricerche in un ambiente multibyte e per le ricerche con caratteri jolly.

Corrispondenza con espressione regolare non trovata

Include le informazioni sugli eventi che non corrispondono a uno o più dei caratteri di espressione regolare immessi. Questa opzione può essere utilizzata per le ricerche in un ambiente multibyte e per le ricerche con caratteri jolly.

Operatori relazionali

Comprendono le informazioni sugli eventi se sussiste la relazione appropriata tra la colonna e il valore immesso. Sono disponibili i seguenti operatori relazionali:

- Uguale a (numerico)
- Diverso da (numerico)
- Maggiore di (numerico)
- Maggiore o uguale a (=>)
- Minore di (numerico)
- Minore o uguale a (=>)

Ad esempio, l'operatore *Maggiore di* include le informazioni sugli eventi dalla colonna selezionata se il relativo valore è maggiore del valore impostato.

Tutti questi operatori consentono di individuare solo numeri; per cercare altri caratteri, selezionare gli operatori "corrispondenza" come appropriato.

Modalità di creazione di una regola per il riepilogo

È possibile utilizzare le regole di riepilogo per combinare alcuni eventi nativi di tipo comune in un unico evento perfezionato. Questo consente di risparmiare spazio nell'archivio registro eventi e semplifica l'analisi degli eventi.

Ad esempio, è possibile creare una regola per il riepilogo che registri un singolo evento perfezionato ogni tre tentativi di accesso falliti dallo stesso utente. Questo significa che l'archivio registro eventi memorizza soltanto un evento invece di tre.

La creazione o di modifica di una regola per il riepilogo tramite la relativa procedura guidata si articola nei passaggi seguenti:

1. Apertura della procedura guidata regola di riepilogo
2. Soglie di riepilogo: impostazione del numero o della frequenza di eventi nativi da raccogliere in un evento di riepilogo.
3. Selezione evento: identificazione di un evento di cui eseguire il riepilogo tramite gli attributi di normalizzazione CEG e i filtri avanzati facoltativi.
4. Riepilogo: controllo della modalità in cui l'evento di riepilogo finale verrà presentato nei rapporti.

Nota: una volta creata una regola per il riepilogo, occorre applicarla perché sia utilizzabile nel proprio ambiente.

Ulteriori informazioni

Apertura della procedura guidata di riepilogo (a pagina 527)
Impostazione delle soglie di riepilogo (a pagina 528)
Configurazione di una visualizzazione di riepilogo (a pagina 531)
Applicazione di una regola di soppressione o riepilogo (a pagina 533)

Apertura della procedura guidata di riepilogo

Per creare una nuova regola di riepilogo o modificarne una esistente, aprire la procedura guidata di riepilogo.

Per aprire la procedura guidata di soppressione

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Raccolta registri.

   Viene visualizzato l'elenco della cartella Raccolta registri.

2. Fare clic sulla freccia accanto alla cartella Libreria di perfezionamento eventi per espanderla; quindi, selezionare la cartella Soppressione e riepilogo.

   Nel riquadro dei dettagli vengono visualizzati i pulsanti per la soppressione e il riepilogo.

3. Fare clic su Nuova regola di riepilogo:

   Viene visualizzata la procedura guidata di riepilogo.

   Mentre si utilizza la procedura guidata:

   - Fare clic su Salva per salvare il file della regola senza chiudere la procedura.
   - Fare clic su Salva e chiudi per salvare il file della regola e chiudere la procedura.
   - Fare clic su Ripristina per ripristinare la visualizzazione della procedura alle ultime impostazioni salvate.

Ulteriori informazioni

Impostazione delle soglie di riepilogo (a pagina 528)
Configurazione di una visualizzazione di riepilogo (a pagina 531)

Impostazione delle soglie di riepilogo

Per creare o modificare una regola di riepilogo, inserire le informazioni generali e impostare le soglie di riepilogo. Le soglie sono un numero di eventi, una frequenza di occorrenza o la combinazione delle due cose, che danno il via alla creazione di un evento di riepilogo.

Per impostare le soglie di riepilogo

1. Aprire la procedura guidata di riepilogo.
2. Immettere un nome per la nuova regola. È inoltre possibile immettere informazioni descrittive facoltative di riferimento.
3. Definire la combinazione specificando il numero di eventi nativi e il tempo trascorso che la regola utilizza per creare un singolo evento perfezionato utilizzando i menu di Riepilogo eventi:

   Abilita soglia conteggio eventi

   Controlla se la regola utilizza o meno una soglia evento. Il valore della soglia evento deve essere superiore a uno. La selezione di questa casella imposta il valore massimo degli eventi. Se la casella è deselezionata e il periodo di timeout degli eventi è attivo, soltanto il periodo di tempo viene considerato nel riepilogo degli eventi. Se sono abilitate entrambe le opzioni, viene creato un evento di riepilogo proprio nel periodo di tempo specificato, purché si verifichi almeno un evento non elaborato qualificato.

   N. massimo di eventi

   Indica il numero di eventi nativi che avviano un evento di riepilogo. Quando si verifica il numero di eventi nativi specificato, si crea un evento di riepilogo.

   Minimo: 2

   Massimo: 5000

   Abilita periodo di timeout eventi

   Controlla se la regola utilizza o meno una soglia di periodo di tempo. La selezione di questa casella imposta il valore di un periodo di tempo. Se la casella non è selezionata, si verifica un evento di riepilogo soltanto quando viene raggiunta la soglia del conteggio eventi.

Periodo di tempo

Definisce, in secondi, il tempo che occorre per avviare un evento di riepilogo, se si sono verificati eventi del tipo specificato. Quando viene raggiunta la soglia, si verifica la creazione di un evento di riepilogo, purché si sia verificato almeno un evento nativo qualificato. È possibile impostare il periodo di tempo a zero, in modo da avere come risultato un evento di riepilogo soltanto quando viene raggiunta la soglia massima di eventi.

Minimo: 0

Massimo: 86400

Ad esempio, nel caso di una regola che riepiloghi i tentativi di accesso falliti, la selezione di 3 nel menu N. massimo di eventi e di 10 nel menu Periodo di tempo ha come risultato il riepilogo dell'evento dopo tre tentativi di accesso falliti oppure ogni 10 secondi, purché si verifichi almeno un accesso fallito.

4. Fare clic sulla freccia appropriata per andare al passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, la nuova regola viene visualizzata nell'elenco; altrimenti, appare il passaggio selezionato.

Ulteriori informazioni

Configurazione di una visualizzazione di riepilogo (a pagina 531)

Selezione di un evento di riepilogo

Specificare l'evento nativo che la regola dovrà riepilogare impostando un filtro semplice per i campi di normalizzazione eventi CEG. Questi quattro campi, che fanno parte della classe specifica di ogni evento, vengono forniti per tutti gli eventi espressi nella CEG e consentono di identificare con precisione un evento.

È possibile specificare la combinazione di campi di normalizzazione eventi desiderata utilizzando la scheda Filtri semplici. È inoltre possibile utilizzare i filtri avanzati per ulteriori dettagli sull'identificazione di eventi. Specificare almeno un filtro semplice per una regola di soppressione.

Per selezionare un evento regola di riepilogo

1. Aprire la procedura guidata di riepilogo e andare al passaggio Filtraggio.
2. Creare i filtri semplici per selezionare l'evento desiderato selezionando la casella di controllo corrispondente e selezionando o inserendo il valore desiderato. Di seguito sono elencati i campi disponibili:

   Modello ideale

   Descrive l'ampia classe di tecnologie coinvolte nell'evento. Ad esempio, Firewall e Dispositivo di rete sono modelli ideali.

   Categoria evento

   Descrive ampie categorie di eventi. Per esempio tutti gli eventi relativi ad account, gruppi utenti e ruoli sono registrati nella categoria di eventi "Gestione identità". Ogni categoria di eventi dispone di una o più classi (sottocategorie), quindi qualsiasi scelta modifica le selezioni disponibili nel menu Classe di eventi.

   Classe evento

   Consente una classificazione più dettagliata degli eventi di una categoria specifica. Ad esempio, gli eventi Gestione identità sono divisi in una di tre classi: account, gruppo o identità. Ad ogni classe di evento sono associate una o più azioni, quindi qualsiasi scelta modifica le selezioni disponibili nel menu Azioni evento.

   Azione evento

   Descrive azioni comuni per ogni categoria e classe di eventi. Ad esempio, Gestione account, una classe della categoria Gestione identità, contiene le azioni di creazione, eliminazione e modifica dell'account.
3. Fare clic sulla freccia appropriata per andare al passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

Facendo clic su Salva e chiudi, nell'elenco verrà visualizzata la nuova regola. In alternativa, apparirà il passaggio selezionato.

Ulteriori informazioni:

Creazione di un filtro evento semplice (a pagina 584)
Creazione di un filtro di eventi avanzato (a pagina 586)
Configurazione di una visualizzazione di riepilogo (a pagina 531)
Impostazione delle soglie di riepilogo (a pagina 528)

Configurazione di una visualizzazione di riepilogo

Le regole di riepilogo controllano il modo in cui gli eventi nativi vengono visualizzati nell'evento elaborato. È possibile configurare una visualizzazione di riepilogo selezionando Riepilogo per Campi e Campi aggregati.

Per configurare la visualizzazione di una regola di riepilogo

1. Aprire la procedura guidata di riepilogo e andare al passaggio Riepilogo.
2. Selezionare il campo o i campi secondo i quali riepilogare gli eventi tramite il controllo pilota:

   Riepilogo per

   Controlla il campo o i campi in base ai quali viene raggruppata l'informazione riepilogata. Ad esempio, nel caso di una regola di riepilogo degli accessi falliti, selezionare source_username per visualizzare il numero degli eventi di accesso non riusciti qualificati per ogni utente univoco. Per completare la regola, occorre selezionare uno o più campi Riepilogo per.

3. (Facoltativo) Selezionare il campo o i campi per i quali si vuole sia aggregato l'evento elaborato.

   Aggregato

   Controlla il campo o i campi secondo cui sono suddivise le informazioni riepilogate, secondo il campo Riepilogo per. Ad esempio, nel caso di una regola che riepiloghi gli accessi non riusciti, selezionare source_username come campo Riepilogo per e dest_hostname come campo Aggregato. In questo modo viene visualizzato il numero di eventi di accesso non riusciti qualificati per ogni utente unico, suddivisi per l'host al quale l'utente ha tentato di accedere.

   Le informazioni relative ai campi aggregati vengono mantenute nel campo evento non elaborato degli eventi di riepilogo. Nell'esempio precedente, ogni host unico al quale l'utente ha cercato di effettuare l'accesso verrà archiviato assieme al numero di occorrenze nel formato seguente: *nomehost1:2,nomehost2:5*. Questo esempio indica due tentativi di accesso dall'host 1 e cinque tentativi dall'host 2.

   I campi aggregati sono facoltativi, quindi non è necessario selezionare un campo aggregato per completare la regola.

4. Fare clic sulla freccia appropriata per andare al passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, la nuova regola viene visualizzata nell'elenco; altrimenti, viene visualizzato il passaggio selezionato.

Quando viene creata una nuova regola, essa viene salvata come versione 1.0. Se in seguito la regola viene modificata, una copia separata di essa viene memorizzata come nuova versione. È possibile visualizzare le versioni precedenti e applicarle o copiarle, secondo necessità.

Ulteriori informazioni

Impostazione delle soglie di riepilogo (a pagina 528)

Applicazione di una regola di soppressione o riepilogo

Una volta creata una regola per la soppressione o il riepilogo, occorre applicarla perché sia utilizzabile nel proprio ambiente. Questa funzione aiuta a impedire l'applicazione di regole di soppressione o riepilogo senza un'adeguata verifica e la relativa approvazione.

Per applicare una regola di soppressione o riepilogo

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.

   Viene visualizzato l'Elenco servizi.

2. Fare clic sull'icona Archivio registro eventi.

   Viene visualizzato il riquadro di configurazione dell'archivio registro eventi.

3. Individuare e selezionare la regola di soppressione o riepilogo che si desidera applicare tramite il relativo controllo pilota.

4. Fare clic su Salva.

   Viene visualizzato un messaggio che conferma l'applicazione corretta della regola.

Come applicare regole di soppressione e riepilogo ai componenti degli agenti

È possibile assegnare regole di soppressione, riepilogo o entrambi i tipi di regole ai gruppi di agenti, agli agenti o ai connettori presenti nel proprio ambiente. Queste regole possono sostituire o completare qualsiasi regola di soppressione o riepilogo applicata al server di CA User Activity Reporting Module. Pertanto, è possibile semplificare il processo di trasmissione/ricezione degli eventi controllando dove avverrà il perfezionamento.

Ad esempio, se si dispone di un gruppo di agenti di Windows, è possibile associare una regola di soppressione per eliminare gli eventi di Windows non necessari agli agenti del gruppo. In questo modo, non è più necessario sottoporre tutti gli eventi in arrivo ad un controllo specifico di Windows sul server CA User Activity Reporting Module.

È possibile applicare le regole di soppressione e riepilogo a livelli differenti della gerarchia delle cartelle degli agenti:

- Dalla cartella Explorer agente è possibile applicare le regole ad un qualsiasi gruppo di agenti, ai singoli agenti o ai connettori.
- Dalla cartella di un gruppo di agenti specifico è possibile applicare le regole a tutti gli agenti contenuti nel gruppo e a tutti i connettori assegnati ad essi.
- Da un singolo agente è possibile applicare le regole solo all'agente in questione e ai connettori ad esso assegnati.

Il processo di applicazione delle regole di soppressione o riepilogo ai componenti degli agenti è composto dai passaggi seguenti:

1. Aprire la procedura guidata di gestione delle regole.
2. Selezionare le destinazioni: gruppi di agenti, agenti o connettori.
3. Selezionare le regole di soppressione da applicare.
4. Selezionare le regole di riepilogo da applicare.

Utilizzando la procedura guidata di gestione delle regole, è anche possibile eliminare le regole di soppressione o di riepilogo da più gruppi di agenti, agenti o connettori.

Ulteriori informazioni:

Aprire la procedura guidata Gestisci regole di riepilogo. (a pagina 534)
Selezionare le destinazioni di soppressione e riepilogo (a pagina 535)
Selezione delle regole di soppressione da applicare (a pagina 535)
Selezionare le regole di riepilogo da applicare (a pagina 536)

Aprire la procedura guidata Gestisci regole di riepilogo.

Per applicare le regole di soppressione o riepilogo a gruppi di agenti, singoli agenti o connettori, è possibile utilizzare la procedura guidata di gestione delle regole.

Per aprire la procedura guidata di gestione delle regole

1. Fare clic sulla scheda Amministrazione, e quindi sulla sottoscheda Raccolta registri.

   Verrà visualizzato l'elenco cartella di Raccolta registri.

2. Fare clic sulla cartella Explorer agente e quindi su Gestione regole di soppressione e di riepilogo:

   Verrà visualizzata la procedura guidata di gestione delle regole.

   Quando si utilizza la procedura guidata:

   - Fare clic su Salva per memorizzare il file senza chiudere la procedura guidata.
   - Fare clic su Salva e chiudi per salvare il file e chiudere la procedura guidata.
   - Fare clic su Reimposta per ripristinare la visualizzazione della procedura guidata alle ultime impostazioni salvate.

Selezionare le destinazioni di soppressione e riepilogo

Per applicare le regole di soppressione o riepilogo ai componenti degli agenti, selezionare le destinazioni per tali regole.

Per selezionare le destinazioni

1. Aprire la procedura guidata di gestione delle regole.
2. Selezionare se applicare le regole ai gruppi di agenti, agli agenti o ai connettori.
3. (Facoltativo) Selezionare Elimina per eliminare le regole anziché aggiungerle.
4. Selezionare le destinazioni tramite il controllo pilota.

   Nota: è possibile eseguire la ricerca in base al nome dell'agente o del connettore. Se nell'elenco disponibile non compaiono né agenti né connettori, fare clic su Cerca per visualizzare tutti gli agenti o connettori disponibili.
5. Avanzare al passaggio di applicazione delle regole, se necessario.

Selezione delle regole di soppressione da applicare

Per completare l'assegnazione delle regole di soppressione a un gruppo di agenti, a un agente o a un connettore, selezionare quali regole applicare.

Per scegliere le regole di soppressione

1. Aprire la procedura guidata di applicazione delle regole di soppressione e andare al passaggio Applica regole di soppressione.

2. Scegliere quali, tra le regole disponibili, applicare tramite il controllo pilota.

   Nota: è possibile cercare le regole di soppressione tramite il campo Modello regole di soppressione.

3. Fare clic su Salva e chiudi.

   Le regole selezionate vengono applicate alle destinazioni scelte.

Selezionare le regole di riepilogo da applicare

Per completare l'assegnazione delle regole di riepilogo ad un gruppo di agenti, ad un agente o ad un connettore, selezionare le regole da applicare.

Per selezionare le regole di riepilogo

1. Aprire la procedura guidata di applicazione delle regole di riepilogo e accedere al passaggio Applica regole di riepilogo.
2. Utilizzando il controllo pilota, selezionare le regole da applicare tra quelle disponibili.

   Nota: è possibile ricercare le regole di riepilogo utilizzando il campo Modello regole di riepilogo.

3. Fare clic su Salva e chiudi dopo aver completato l'applicazione delle regole.
4. Le regole selezionate vengono applicate alle destinazioni scelte. Selezionando Elimina al passaggio Selezionare destinazioni, le regole selezionate verranno eliminate.

Copia di una regola di soppressione o riepilogo

È possibile copiare una regola di soppressione o riepilogo, in modo da poter creare una nuova regola sulla base di una esistente.

Per copiare una regola di soppressione o riepilogo

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Raccolta registri.

   Viene visualizzato l'elenco della cartella Raccolta registri.

2. Fare clic sulla freccia accanto alla cartella Libreria di perfezionamento eventi per espanderla; quindi, selezionare la cartella Soppressione e riepilogo.

   Nel riquadro dei dettagli viene visualizzato il pulsante per la soppressione e il riepilogo.

3. Fare clic sulla cartella Soppressione e riepilogo contenente la regola da copiare.

   La cartella si apre, mostrando le regole.

4. Selezionare la regola da copiare e fare clic su Copia elemento selezionato:

   Viene visualizzata la procedura guidata di soppressione o riepilogo, che mostra la regola.

5. Apportare le modifiche desiderate, quindi fare clic su Salva e chiudi.

   La regola viene visualizzata nell'elenco appropriato.

Modifica di una regola per la soppressione o il riepilogo

È possibile modificare una regola per la soppressione o il riepilogo.

Per modificare una regola per la soppressione o il riepilogo

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Raccolta registri.

   Viene visualizzato l'elenco della cartella Raccolta registri.

2. Fare clic sulla freccia accanto alla cartella Libreria di perfezionamento eventi per espanderla; quindi, selezionare la cartella Soppressione e riepilogo.

   Nel riquadro dei dettagli vengono visualizzati i pulsanti per la soppressione e il riepilogo.

3. Fare clic sulla cartella Soppressione e riepilogo contenente la regola da modificare.

4. Selezionare la regola da modificare e fare clic sull'icona Modifica regola di soppressione o di riepilogo.

   Vengono visualizzate le procedure guidate di soppressione o di riepilogo, che mostrano la regola selezionata.

5. Apportare le modifiche desiderate, quindi fare clic su Salva e chiudi.

   La regola appare nell'elenco appropriato come nuova versione della regola modificata.

Ulteriori informazioni

Versioni dei componenti per il perfezionamento degli eventi (a pagina 517)

Eliminazione di una regola per la soppressione o il riepilogo

È possibile eliminare una regola per la soppressione o il riepilogo non più necessaria.

Per eliminare una regola per la soppressione o il riepilogo

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Raccolta registri.

   Viene visualizzato l'elenco della cartella Raccolta registri.

2. Fare clic sulla freccia accanto alla cartella Libreria di perfezionamento eventi per espanderla; quindi, selezionare la cartella Soppressione e riepilogo.

   Nel riquadro dei dettagli vengono visualizzati i pulsanti per la soppressione e il riepilogo.

3. Fare clic sulla cartella Soppressione e riepilogo contenente la regola da eliminare.

4. Selezionare la regola da eliminare e fare clic sull'icona Elimina regola di soppressione o di riepilogo. La versione corrente è selezionata per impostazione predefinita. È possibile selezionare una versione precedente da rimuovere dall'elenco a discesa Versione situato nel riquadro dei dettagli.

   Viene visualizzata una finestra di dialogo di conferma. Se la regola è stata applicata a un'integrazione, verrà visualizzato un avviso. L'eliminazione della regola la rimuove anche dall'integrazione.

5. Fare clic su Sì.

   La regola eliminata viene rimossa dall'elenco appropriato.

Importazione di una regola per la soppressione o il riepilogo

È possibile importare una regola per la soppressione o il riepilogo, in modo da poter spostare le regole da un ambiente all'altro. Ad esempio, è possibile importare nel proprio ambiente attivo le regole create in un ambiente di prova.

Per importare una regola di soppressione o riepilogo

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Raccolta registri.

   Viene visualizzato l'elenco della cartella Raccolta registri.

2. Fare clic sulla freccia accanto alla cartella Libreria di perfezionamento eventi per espanderla; quindi, selezionare la cartella Soppressione e riepilogo.

   Nel riquadro dei dettagli vengono visualizzati i pulsanti Importa regola per la soppressione e riepilogo ed Esporta regola per la soppressione o riepilogo.

3. Fare clic su Importa regola per la soppressione o il riepilogo.

   Viene visualizzata la finestra di dialogo per l'importazione del file.

4. Selezionare il file da importare, quindi fare clic su OK.

   Vengono visualizzate le procedure guidate di soppressione o riepilogo contenenti i dettagli della regola selezionata.

5. Apportare le modifiche desiderate, quindi fare clic su Salva e chiudi. Se la regola importata ha lo stesso nome di una che si trova già nel database di gestione, verrà richiesto di modificare il nome.

   La regola importata appare nella cartella di soppressione o riepilogo adeguata.

Esportazione di una regola per la soppressione o il riepilogo

È possibile esportare una regola per la soppressione o il riepilogo, in modo da poter condividere le regole tra ambienti diversi. Ad esempio, è possibile esportare nel proprio ambiente attivo le regole create in un ambiente di prova.

Per esportare una regola per la soppressione o il riepilogo

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Raccolta registri.

   Viene visualizzato l'elenco della cartella Raccolta registri.

2. Fare clic sulla freccia accanto alla cartella Libreria di perfezionamento eventi per espanderla; quindi, selezionare la cartella Soppressione e riepilogo.

   Il pulsante Esporta regola di soppressione o di riepilogo viene visualizzato nel riquadro dei dettagli.

3. Fare clic sulla cartella Regole per la soppressione o Regole per il riepilogo che contiene il file da esportare.

   La cartella si espande e mostra i file individuali.

4. Selezionare la regola da esportare, quindi fare clic su Esporta regola di soppressione o di riepilogo. La versione corrente è selezionata per impostazione predefinita. È possibile selezionare una versione precedente da esportare dall'elenco a discesa Versione situato nel riquadro dei dettagli.

   Viene visualizzata la finestra di dialogo relativa alla posizione dell'esportazione.

5. Inserire o selezionare la posizione in cui archiviare la regola esportata e fare clic su Salva.

   Viene visualizzata una finestra di dialogo che conferma l'avvenuta esportazione.

6. Fare clic su OK.

   La regola viene esportata.

Creazione di una regola di soppressione per l'evento Windows 560

L'abilitazione del controllo degli accessi agli oggetti su un server Windows crea un volume significativo di traffico di eventi, alcuni dei quali probabilmente da eliminare. Ad esempio, Windows genera due eventi ogni volta che un amministratore apre Microsoft Management Console (mmc.exe). I valori ID di questi eventi sono 560 e 562.

In questo esempio, viene creata una nuova regola che elimina gli eventi Windows con un event_id di 560. Il completamento dei passaggi della seguente procedura fornisce una vera regola di soppressione da utilizzare nel proprio ambiente di rete, oltre a una dimostrazione dell'utilizzo della procedura guidata.

Per iniziare con questo esempio, accedere a un server CA User Activity Reporting Module come utente con ruolo e privilegi di amministratore. Non è possibile creare o modificare regole di soppressione quando si accede come utente EiamAdmin.

Per creare una regola di soppressione per gli eventi Windows 560

1. Aprire la procedura guidata regola di soppressione.
2. Inserire "Soppressione dell'evento Windows 560" nel campo di immissione del nome e aggiungere la descrizione: "Questa regola sopprime l'evento Windows 560 dato che il sistema operativo crea anche l'evento 562 per lo stesso tipo di accesso alla risorsa. La sua memorizzazione non è necessaria per la dimostrazione di compatibilità".
3. Proseguire fino al passaggio Filtro e selezionare i seguenti filtri semplici:
   a. Valore modello ideale, Sistema operativo.
   b. Valore categoria evento, Accesso alla risorsa.
   c. Valore classe evento, Apertura risorse.
   d. Valore azione evento, Attività risorse.

4. Fare clic sulla scheda Filtri avanzati, quindi sul pulsante Nuovo filtro evento.

   Nella tabella viene visualizzata una nuova riga relativa al filtro. È possibile fare clic su un valore o su uno spazio vuoto in ogni cella della tabella per selezionare o inserire un nuovo valore.

   Il campo Operatore logico ha come valore predefinito AND. Se vi sono diversi tipi di eventi da eliminare, è possibile inserire i relativi ID evento con nuove righe che utilizzano l'operatore logico OR.

5. Impostare i valori del campo Filtri avanzati:

   a. Fare clic sul valore nel campo Colonna e selezionare il campo event_id.

   b. Fare clic sul campo Operatore e selezionare Uguale a.

   c. Fare clic sul campo Valore e inserire il valore 560.

6. Fare clic su Salva e chiudi.

   La procedura guidata crea automaticamente una cartella Utente per contenere le regole di soppressione. Questa cartella può essere visualizzata espandendo la cartella Regole per la soppressione.

Capitolo 15: Mapping e Analisi

Questa sezione contiene i seguenti argomenti:

Stati evento (a pagina 546)
Attività relative a regole di mapping e analisi (a pagina 548)
Modalità di creazione di un file di analisi del messaggio (a pagina 548)
Modalità di creazione di un file di mapping dei dati (a pagina 568)
Attività delle regole di inoltro eventi (a pagina 581)

Stati evento

Le informazioni sugli eventi nel proprio ambiente passano attraverso una serie di passaggi, dall'occorrenza iniziale alla possibile visualizzazione finale in CA User Activity Reporting Module. Dal momento che il termine "evento" può riferirsi a uno qualunque di questi passaggi, per i possibili stati degli eventi nell'ambiente viene utilizzata la seguente terminologia:

Evento nativo

Fa riferimento all'occorrenza originale dello stato o azione che attiva l'evento, ad esempio un'autenticazione non riuscita o una violazione del firewall. Gli eventi nativi vengono inviati dal connettore o dal servizio listener appropriato, opportunamente analizzati e mappati, e quindi inseriti nell'archivio di registro eventi, dove sono disponibili per la visualizzazione come eventi non elaborati e/o perfezionati.

Evento non elaborato

Si riferisce alla comunicazione inviata dall'agente di monitoraggio appropriato. Gli eventi non elaborati contengono informazioni relative all'evento nativo, spesso sotto forma di stringa syslog o di coppia nome-valore. Queste informazioni sono archiviate e ricercabili, a meno che vengano alterate da regole di soppressione o riepilogo. Gli eventi soppressi non vengono registrati nell'archivio registro eventi; un gruppo di eventi riepilogati viene registrato come singolo evento che esprime il risultato dell'operazione di riepilogo.

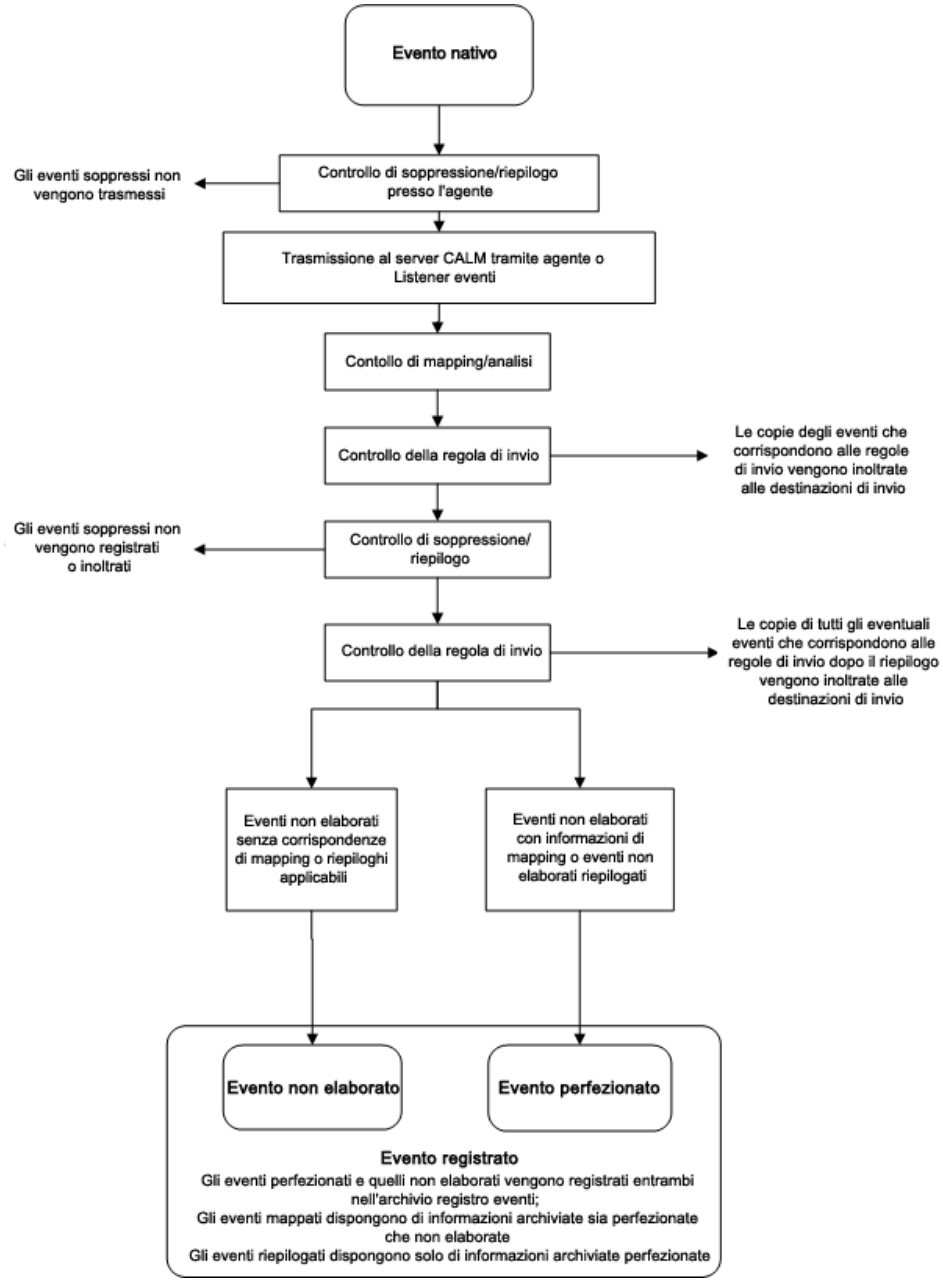
Evento perfezionato

Si riferisce alle informazioni di evento mappate e riepilogate da CA User Activity Reporting Module. Si tratta di informazioni memorizzate e ricercabili.

Evento registrato

Si riferisce alle informazioni sull'evento non elaborato o perfezionato nell'archivio registro eventi. Gli eventi non elaborati e quelli perfezionati vengono sempre registrati, a meno che vengano eliminati o riepilogati. Per gli eventi mappati sono disponibili informazioni non elaborate e perfezionate. Si tratta di informazioni memorizzate e ricercabili.

Per informazioni sullo stato degli eventi, consultare il diagramma seguente:



Ulteriori informazioni:

Attività relative alle regole per la soppressione e il riepilogo (a pagina 518)
Attività relative a regole di mapping e analisi (a pagina 548)

Attività relative a regole di mapping e analisi

I file di analisi del messaggio (XMP) e di mapping dei dati (DM) raccolgono e normalizzano i dati da tipi specifici di origini evento. La maggior parte degli eventi nativi in arrivo passa attraverso i processi di analisi e di mapping per creare un evento segnalabile inserito nell'archivio registro eventi. Gli eventi trasmessi tramite SAPI o iTechnology non richiedono analisi e passano direttamente alla fase di mapping dei dati.

Nota: per sfruttare pienamente queste funzioni avanzate, è necessario avere una conoscenza approfondita degli eventi non elaborati e raccolti all'interno del proprio ambiente, dei campi che si desidera analizzare, della sintassi dell'espressione regolare, della CEG e dei file XMP e DM, oltre che del modo in cui vengono analizzati gli eventi.

I file XMP basati su XML leggono gli eventi non elaborati in arrivo e creano coppie nome-valore in base alle specifiche definite. Dopodiché, i file DM mappano le coppie nome-valore degli eventi, assegnate tramite l'analisi dei messaggi, nella Common Event Grammar. Quando si creano nuovi file di analisi e mapping, occorre considerarli come parte di un processo. Ad esempio, un'analisi completa ed efficiente consente un mapping rapido ed efficace ai fini della procedura.

Ulteriori informazioni

Versioni dei componenti per il perfezionamento degli eventi (a pagina 517)
Modalità di creazione di un file di analisi del messaggio (a pagina 548)
Modalità di creazione di un file di mapping dei dati (a pagina 568)

Modalità di creazione di un file di analisi del messaggio

È possibile utilizzare la procedura guidata file di analisi per creare, modificare o analizzare un file di analisi del messaggio (XMP). I file di analisi leggono i dati degli eventi non elaborati in arrivo e creano coppie nome-valore, consentendo di definire il mapping persino prima del processo di mapping dei dati. In questo modo si migliora l'efficienza globale del mapping.

Nota: i nomi della Common Event Grammar (CEG) non vengono implementati per l'analisi degli eventi e consentono una flessibilità aggiuntiva nella creazione delle coppie nome-valore. I campi CEG sono disponibili per la selezione, ma i loro nomi e valori non si limitano ai valori CEG.

La creazione o modifica di un file XMP prevede i passaggi seguenti:

1. Apertura della procedura guidata file di analisi.
2. Fornitura di dettagli sul file, tra cui nome file, nome registro e informazioni di supporto.
3. Individuazione di eventi di esempio per la verifica e la costruzione dei file.
4. Impostazione di valori globali che si applicheranno a tutti gli eventi analizzati dal file.
5. Creazione o modifica di stringhe di corrispondenza preliminare per avviare l'analisi dell'evento
6. Selezione dei filtri di corrispondenza preliminare per l'analisi degli allegati ai filtri.
7. Creazione o modifica dei filtri di analisi per il completamento dell'analisi evento.
8. Analisi e salvataggio del file XMP nuovo o modificato.

Ulteriori informazioni

Definizione dei dettagli del file (a pagina 550)
Caricamento di eventi campione (a pagina 552)
Aggiungi campi globali (a pagina 553)
Creazione di un filtro di corrispondenza preliminare (a pagina 554)
Analisi del file XMP (a pagina 567)

Apertura della procedura guidata file di parsing

Per creare una regola di parsing del messaggio o modificarne una esistente, è necessario aprire la procedura guidata file di parsing.

Per aprire la procedura guidata file di parsing

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria.
2. Fare clic sulla freccia accanto a alla cartella Integrazione Log per espanderla, quindi selezionare la cartella Mapping e parsing.

   I pulsanti di integrazione del prodotto vengono visualizzati nel riquadro dei dettagli.

3. Fare clic su Nuova regola di parsing del messaggio:

   Viene aperta la procedura guidata file di parsing.

   Quando si utilizza la procedura guidata:

   - Fare clic su Salva per salvare la procedura guidata senza chiuderla.
   - Fare clic su Salva e chiudi per salvare il file e chiudere la procedura guidata.
   - Fare clic su Reimposta per ripristinare la visualizzazione della procedura guidata alle ultime impostazioni salvate.

Definizione dei dettagli del file

È possibile aggiungere nuovi dettagli per l'analisi dei file, tra cui informazioni su nome, origine e riferimento. I file appena creati o modificati vengono visualizzati nella cartella Utente nell'area Mapping e Analisi.

Per aggiungere nuovi dettagli al file di analisi

1. Aprire la procedura guidata file di analisi.
2. Specificare le informazioni sul file di analisi nell'area relativa come indicato nella sottoprocedura seguente:
   a. Digitare un nome per il file. Il nome del file è obbligatorio e non può contenere i caratteri: / \ : * ? “ < > ^;'`,&{}[]. o |.
   b. Inserire il nome registro di origine per identificare il nome registro del tipo di evento da analizzare. La funzione di completamento automatico presenta i nomi registro disponibili durante la digitazione. Il nome registro selezionato verrà visualizzato nel campo event_logname dell'evento perfezionato.
   c. Se occorre, aggiungere una descrizione come riferimento.
3. (Facoltativo) Aggiungere informazioni di supporto come riferimento secondo quanto indicato nei passaggi secondari che seguono.
   a. Fare clic su Aggiungi prodotto nell'area Informazioni di supporto.

      Viene visualizzata una nuova riga con le informazioni di supporto.
   b. Fare clic sul testo Nuovo prodotto o Nuova versione per abilitare i campi di immissione e digitare le informazioni desiderate sul prodotto e/o sulla versione.
4. Fare clic sulla freccia appropriata per passare al passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, il nuovo file viene visualizzato nella cartella Utente file di analisi; altrimenti, verrà visualizzato il passaggio selezionato.

Caricamento di eventi campione

È possibile fornire eventi campione da utilizzare nella verifica del nuovo file XMP effettuando una ricerca tramite l'archivio registro eventi o l'accesso a un file di registro. Gli eventi campione forniscono un modello a fronte del quale verificare il file di analisi mentre lo si crea negli altri passaggi della procedura guidata. È anche possibile utilizzare gli eventi campione per verificare l'output di analisi nell'ultimo passaggio della procedura guidata.

Per fornire esempi campione

1. Aprire la procedura guidata file di analisi e avanzare fino al passaggio Caricamento eventi.

   Verrà visualizzata la schermata Caricamento eventi.

2. Selezionare il pulsante di opzione Archivio di registro o File di registro nell'area Trova eventi campione.

   - Se si seleziona Archivio di registro:

     a. Scegliere il tipo di origine evento campione desiderato dal menu a discesa Colonna di analisi. Selezionare result_string per le origini evento WMI, oppure raw_event per le origini evento syslog.

     b. Selezionare la query da utilizzare per fornire eventi campione tramite il filtro tag query e l'elenco query.

     Viene visualizzata la query, che mostra eventi campione che è possibile utilizzare per verificare l'analisi mentre si procede con la procedura guidata.

     Nota: è possibile utilizzare tutte le query disponibili o personalizzate per individuare gli eventi campione. Se si prevede di utilizzare una query personalizzata, è consigliabile crearla e testarla prima di iniziare la procedura di progettazione del file di analisi del messaggio. È consigliabile utilizzare un file evento campione con meno di 1500 eventi per facilitare l'analisi.

   - Se si seleziona File di registro, individuare il file di registro desiderato e fare clic su Carica.

     Gli eventi provenienti dal file di registro vengono visualizzati nel pannello Eventi campione. È possibile utilizzare gli eventi per verificare l'analisi mentre si procede tra i vari passaggi della procedura guidata.

     Nota: la procedura guidata presume che ogni riga del file sia un evento. Gli eventi su più righe non sono supportati.

3. Fare clic sulla freccia appropriata per passare al passaggio della procedura guidata che si desidera completare successivamente.

   Se si fa clic su Salva e chiudi, il nuovo file viene visualizzato nella cartella Utente file di analisi; altrimenti, verrà visualizzato il passaggio selezionato.

Aggiungi campi globali

È possibile aggiungere campi globali, ovvero coppie statiche che corrispondono ad un nome campo con un valore specifico. Il processo di analisi aggiunge campi globali a tutti gli eventi analizzati, pertanto è preferibile utilizzarli per valori predefiniti come modello ideale.

Per aggiungere campi globali

1. Aprire la procedura guidata file di analisi e accedere al passaggio Campi globali.

   Appare la schermata Campi globali.

2. Fare clic su Aggiungi campo globale nell'area Campi globali.

   Appare una nuova riga di campo globale nella tabella dei campi, che visualizza le voci Nuovo campo globale e Nuovo valore.

3. Fare clic sul testo Nuovo campo globale per inserire il nome dell'informazione che si desidera. La funzione di completamento automatico presenta i nomi di campi CEG disponibili mentre si digita. È possibile fare clic su uno di essi per selezionarlo, oppure digitare un nome di campo diverso da quelli CEG.

4. Fare clic sul testo Nuovo valore per inserire il nome dell'informazione che si desidera.

5. (Facoltativo) Ripetere i passaggi 2 e 4 per aggiungere ulteriori campi globali secondo necessità.

6. Fare clic sulla freccia appropriata per andare al passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Facendo clic su Salva e chiudi, nell'elenco della cartella Utente file di analisi verrà visualizzato il nuovo file; in caso contrario, verrà visualizzato il passaggio scelto dall'utente.

Creazione di un filtro di corrispondenza preliminare

È possibile creare un filtro di corrispondenza preliminare per aiutare il file XMP a restringere la ricerca delle informazioni sugli eventi da analizzare. Il filtro di corrispondenza preliminare identifica una stringa di testo selezionata per restringere il processo di selezione dell'evento, che viene poi completato dai filtri di analisi. Se si considera il file di analisi come un imbuto, il filtro di corrispondenza preliminare costituisce l'imboccatura e il filtro di analisi il beccuccio.

L'efficienza del processo di analisi dipende dalla precisione del filtro di corrispondenza preliminare. Questo si verifica perché le strette categorie di corrispondenza preliminare riducono lo sforzo di elaborazione richiesto per analizzare gli eventi.

Ad esempio, se si desidera analizzare gli eventi di tentativo di accesso, è possibile creare un filtro di corrispondenza preliminare per eseguire la ricerca del testo "login" e, quindi, aggiungere i filtri di analisi al filtro appropriati.

Nota: l'eliminazione di un filtro di corrispondenza preliminare rimuove anche il filtro o filtri di analisi associati.

Per creare un filtro di corrispondenza preliminare

1. Aprire la Procedura guidata file di parsing e avanzare fino al passaggio Trova corrispondenza e analizza.

   La procedura guidata visualizza tutti i filtri di corrispondenza preliminare esistenti nel relativo elenco. Per ogni filtro viene visualizzato, tra parentesi, un numero di corrispondenze preliminari agli eventi campione.

2. Fare clic su Aggiungi una stringa di corrispondenza preliminare nella parte superiore dell'elenco Filtri di corrispondenza preliminare, oppure selezionare un filtro da modificare.

   Nota: per selezionare un filtro di corrispondenza preliminare, digitare nel campo Cerca i primi caratteri della stringa di corrispondenza preliminare. Vengono visualizzate tutte le stringhe di corrispondenza preliminare che corrispondono ai caratteri immessi. Non è possibile utilizzare i tasti freccia GIÙ e freccia SU per spostare le stringhe di corrispondenza preliminare visualizzate.

3. Inserire il testo che il filtro deve ricercare nel campo di immissione Stringhe di corrispondenza preliminare.

   Gli eventuali eventi campione che corrispondono al testo inserito compaiono immediatamente, assieme al numero di eventi corrispondenti trovati e analizzati.

4. (Facoltativo) Fare clic su Aggiungi corrispondenza preliminare in base agli eventi non corrispondenti per mostrare tutti gli eventi campione non corrispondenti.

   Gli eventuali eventi attualmente non corrispondenti vengono visualizzati nell'area Eventi e forniscono un riferimento semplice per la creazione di un nuovo filtro di corrispondenza preliminare.

5. (Facoltativo) Aggiungere o modificare ulteriori filtri di corrispondenza preliminare secondo necessità.

6. Impostare l'ordine in cui il processo di analisi deve cercare le corrispondenze preliminari tramite le frecce verso l'alto e verso il basso poste accanto all'elenco dei filtri di corrispondenza preliminare. L'impostazione di filtri di corrispondenza preliminare che creino corrispondenze con un maggior numero di eventi più in alto nell'elenco di priorità aumenta l'efficienza del processo di analisi.

7. Fare clic sulla freccia appropriata per andare al passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, il nuovo file viene visualizzato nella cartella Utente file di analisi; altrimenti, verrà visualizzato il passaggio selezionato.

Creazione di un filtro di analisi

È possibile creare un filtro di analisi per definire la modalità di analisi dei dati evento del file XMP. Ogni filtro di analisi è allegato a un filtro di corrispondenza preliminare. Una volta individuata una stringa di corrispondenza preliminare, il processo di analisi utilizza a turno tutti i filtri di analisi allegati a tale corrispondenza per individuare l'informazione specificata. Il processo di analisi restituisce la prima corrispondenza positiva effettuata.

Quando si seleziona il pulsante Aggiungi filtro di analisi nel passaggio Corrispondenza e analisi della procedura guidata di analisi del messaggio, si avvia la procedura guidata di analisi filtro file. Per creare filtri di analisi efficaci, occorre una buona conoscenza della sintassi dell'espressione regolare.

Per creare un filtro di analisi

1. Aprire la procedura guidata di analisi filtro file e digitare il nome del filtro e una descrizione opzionale nella pagina Dettagli filtro.
2. Fare clic su Aggiungi nuovo per aggiungere un valore campo statico da visualizzare in tutti gli eventi analizzati dal filtro.

   Viene visualizzata una riga campo statica che mostra le celle Nuovo campo e Nuovo valore.
3. Inserire una voce nella cella Nuovo campo e una nella cella Nuovo valore. Man mano che si digita nella cella Nuovo campo, la funzione di completamento automatico riduce i nomi dei campi CEG disponibili e presenta un menu di opzioni.
4. (Facoltativo) Ripetere i passaggi 2-3 per aggiungere valori di campo statici secondo necessità.
5. Proseguire fino al passaggio Espressione regolare.

   Viene visualizzata la finestra Prova dell'espressione di analisi, che mostra tutte le espressioni regolari correnti. Subito al di sotto dell'espressione regolare si trova il pannello Evento. Quest'area mostra uno o più eventi campione, se sono stati caricati in precedenza. La procedura guidata può eseguire un test degli eventi rispetto all'espressione regolare man mano creata.
6. Fare clic su Aggiungi/Rimuovi token dalla libreria per visualizzare un elenco di espressioni regolari predefinite da aggiungere per l'utilizzo nel filtro corrente. Selezionare i token da aggiungere all'elenco Token di analisi e fare clic su OK.

7. (Facoltativo) Fare clic su Nuovo token di espressione regolare per creare un Token di analisi ed immettere nel riquadro Dettagli token la sintassi dell'espressione regolare. Ora è possibile creare espressioni personalizzate per il proprio ambiente. Facendo clic su Aggiungi token selezionato alla libreria, nella parte superiore del riquadro Token di analisi, è possibile aggiungere un token personalizzato alla propria libreria locale.

   Nota: quando si crea un nuovo token data/ora, selezionare la casella di controllo "Considera come valore data/ora" per inserire un formato per analizzare il valore dell'ora. Tale valore non influenza il formato di visualizzazione.

8. Aggiungere istruzioni di espressione regolare per il filtro nel campo di immissione Espressione regolare. È possibile trascinare le espressioni dall'elenco Token di analisi. È inoltre possibile digitare o modificare l'espressione direttamente nel campo Espressione regolare.

   Nota: la selezione di un token nell'elenco Token di analisi ne permette la visualizzazione della sintassi dell'espressione regolare nel pannello Dettagli token. È possibile visualizzare il mapping del token di analisi in una data regola per ripeterlo in altre regole di analisi.

9. (Facoltativo) Selezionare la casella di controllo Coppie nome-valore dinamiche se gli eventi di destinazione includono coppie di chiavi che si desidera visualizzare. Per ulteriori informazioni, consultare la sezione "Analisi dinamica".

10. (Facoltativo) Se si desidera utilizzare l'analisi dinamica, inserirne un'espressione nel campo di immissione delle coppie dinamiche. Ad esempio, immettere:

    ```
    (_PAIR_KEY_)=(_PAIR_VALUE_);
    ```

    Verranno visualizzate tutte le coppie distinte dal segno uguale e separate da un punto e virgola. È possibile inserire più espressioni per trovare le coppie visualizzate in altri formati. Per ulteriori informazioni, consultare la sezione Analisi dinamica.

11. Visualizzare in anteprima la modalità di analisi degli eventi campione tramite i pannelli Evento ed Evento analizzato. Durante la modifica dell'espressione regolare del filtro di analisi, il testo delle parti analizzate dell'evento campione è visualizzato in blu, mentre le coppie analizzate dinamicamente sono di colore verde. È possibile verificare l'efficacia dell'analisi.

12. (Facoltativo) Per un'ulteriore verifica, modificare l'evento campione utilizzando le frecce avanti e indietro sotto il riquadro Evento per spostarsi tra gli eventi campione disponibili.

13. Fare clic su Salva e chiudi una volta soddisfatti dell'espressione regolare. È possibile utilizzare Reimposta per riportare l'espressione regolare allo stato iniziale.

    La procedura guidata di analisi filtro file verrà chiusa e sarà possibile tornare al passaggio Trova corrispondenza e analizza della procedura guidata file di analisi.

Ulteriori informazioni:

Analisi dinamica (a pagina 559)
Token di analisi (a pagina 560)
Aggiunta di un token personalizzato alla libreria (a pagina 564)

Analisi dinamica

È possibile utilizzare l'analisi dinamica, che permette la visualizzazione di più coppie nome-valore inalterate. Questa opzione è diversa dall'analisi statica, che estrae i valori e li imposta su CEG o su altri campi predefiniti. L'analisi dinamica è utile quando le applicazioni o i formati registrano i dati evento in coppie di chiavi che si desidera visualizzare inalterate, ossia non analizzate in nomi CEG o altri valori. Inoltre migliora le prestazioni di analisi nei casi in cui è applicabile.

L'espressione regolare che consente l'analisi dinamica contiene quattro elementi:

1. Un indicatore di chiave coppia "(_PAIR_KEY_)"
2. Un indicatore di valore coppia "(_PAIR_VALUE_)"
3. Un separatore chiave-valore tra il valore di coppia e di chiave
4. Un separatore di coppia tra l'intera espressione e l'espressione successiva.

I separatori utilizzati devono corrispondere alla struttura dell'origine evento analizzata. Se l'origine evento utilizza la virgola come separatore, anche l'espressione regolare deve usarla.

Esempio

```
(_PAIR_KEY_)=(_PAIR_VALUE_);
```

In questo esempio, il separatore chiave-valore è "=" e il separatore di coppia è ";"

L'uso di questa espressione dopo altre espressioni regolari consente al file XMP di individuare e visualizzare qualunque coppia di chiavi presente negli eventi analizzati.

Token di analisi

Un token di analisi è un modello di espressione regolare utilizzabile per creare filtri di analisi. CA User Activity Reporting Module include una libreria di token di analisi contenente token di analisi predefiniti. Ad esempio,la funzione _IP_ token imposta l'espressione regolare che analizza il tipico formato di indirizzo IP. Se si desidera utilizzare un filtro di analisi per estrarre un indirizzo IP, inserire il token _IP_ nel filtro anziché creare ogni volta il linguaggio dell'intera espressione regolare.

È possibile creare token personalizzati e aggiungerli alla libreria locale, oppure esportarli per utilizzarli in un altro ambiente CA User Activity Reporting Module. Se si desidera esportare un token personalizzato, è necessario innanzitutto aggiungerlo alla libreria. È possibile importare token personalizzati da un altro ambiente CA User Activity Reporting Module e creare token personalizzati in un ambiente di prova per poi spostarli in un ambiente attivo.

Ulteriori informazioni:

Valori del token Datetime (a pagina 561)
Aggiunta di un token personalizzato alla libreria (a pagina 564)
Rimozione di un token personalizzato dalla libreria (a pagina 565)
Importazione di token di analisi (a pagina 566)
Esportazione di token di analisi (a pagina 567)

Valori del token Datetime

CA User Activity Reporting Module supporta diverse opzioni di sintassi per i token di analisi di Datetime È possibile utilizzare queste opzioni, in formato Datetime, per personalizzare l'aspetto del proprio timbro di Datetime.

Ogni token Datetime può essere composto da uno dei seguenti elementi:

- Un normale carattere (non % o spazio), che viene visualizzato come inserito. Ad esempio, un punto per separare i valori dell'ora.

  oppure

- Una specifica di conversione. Ogni specifica di conversione è composta da un carattere % seguito da un carattere di conversione che definisce l'output di visualizzazione. Ad esempio, %m per visualizzare il mese.

CA User Activity Reporting Module supporta le seguenti specifiche di conversione:

%a oppure %A

Visualizza il nome del giorno della settimana nella lingua locale, in formato completo o abbreviato. In Windows, questa specifica è disponibile solo in Inglese (Stati Uniti).

%b, %B oppure %h

Visualizza il nome del mese nella lingua locale, in formato completo o abbreviato. In Windows, questa specifica è disponibile solo in Inglese (Stati Uniti).

%c

Visualizza l'ora e la data locali.

%C

Visualizza il numero del secolo (0-99).

%d oppure %e

Visualizza il giorno del mese (1-31)

%D

Visualizza la data in stile americano: mese/giorno/anno, l'equivalente di %m/%d/%y.

Nota: la sintassi %m/%d/%y viene utilizzata in Europa. Il formato standard ISO 8601 è %Y-%m-%d.

%H

Visualizza l'ora in formato 24 ore (0-23).

%I

Visualizza l'ora in formato 12 ore (1-12).

%j

Visualizza il numero del giorno nell'anno (1-366).

%m

Visualizza il numero del mese (1-12).

%M

Visualizza il minuto (0-59).

%n

Inserisce uno spazio arbitrario.

%p

Visualizza l'equivalente locale di AM o PM, se esiste.

%r

Visualizza l'ora in formato 12 ore: ore.minuti.secondi, l'equivalente di %I.%M.%S %p. Se nella sezione LC_TIME locale t_fmt_ampm è vuoto, il comportamento non è definito.

%R

Visualizza l'ora in formato 24 ore: ore.minuti, l'equivalente di %H.%M.

%S

Visualizza il secondo (0-60, 60 può presentarsi nel caso di secondi intercalari).

%t

Visualizza uno spazio arbitrario.

%T

Visualizza l'ora in formato 24 ore: ore.minuti.secondi, l'equivalente di %H.%M.%S.

%U

Visualizza il numero della settimana. Il primo giorno della settimana (0-53) è la domenica. La prima domenica di gennaio è il primo giorno della settimana 1.

%w

Visualizza il numero del giorno della settimana (0-6) in cui domenica = 0.

%W

Visualizza il numero della settimana, con il lunedì come primo giorno (0-53). Il primo lunedì di gennaio è il primo giorno della settimana 1.

%x

Visualizza la data utilizzando il formato locale.

%X

Visualizza l'ora utilizzando il formato locale.

%y

Visualizza l'anno del secolo corrente (0-99). Se non si specifica il secolo, i valori dell'intervallo 69-99 si riferiranno agli anni del ventesimo secolo (1969-1999), mentre i valori dell'intervallo 00-68 si riferiranno agli anni del ventunesimo secolo (2000-2068).

%Y

Visualizza l'anno, secolo compreso (ad esempio 1991).

%z

Visualizza una specifica di fuso orario standard RFC-822/ISO 8601. Questa specifica non è disponibile per Windows.

Il formato predefinito del token Datetime di CA User Activity Reporting Module è:

%d/%b/%Y.%H.%M.%S %z

Aggiunta di un token personalizzato alla libreria

È possibile aggiungere token di analisi personalizzati alla libreria dei token per renderli disponibili ad altri utenti. Ad esempio, se durante il processo di creazione del file di analisi dei messaggi si crea un token personalizzato, utile per altre analisi, questo potrà essere aggiunto alla libreria per il successivo riutilizzo.

La seguente procedura presuppone che l'utente aggiunga token durante la creazione dei file o dei filtri di analisi.

Per aggiungere un token di analisi personalizzato alla libreria

1. Aprire la procedura guidata file di analisi dei messaggi e accedere al passaggio Trova corrispondenza e analizza.
2. Aprire la procedura guidata di analisi filtro file e accedere al passaggio Espressione regolare.
3. (Facoltativo) Fare clic su Nuova espressione regolare per creare un Token di analisi ed immettere nel riquadro Dettagli token la sintassi dell'espressione regolare.
4. Selezionare il nuovo token di analisi e fare clic su Aggiungi token selezionato alla libreria.

   Viene visualizzata una finestra di dialogo di conferma.
5. Fare clic su Sì.
6. (Facoltativo) Fare clic su Aggiungi/Rimuovi token dalla libreria per visualizzare il nuovo token.

   Verrà visualizzata la finestra di dialogo della libreria dei token di analisi, con visualizzati in nero i token personalizzati e in verde quelli predefiniti.

Rimozione di un token personalizzato dalla libreria

È possibile rimuovere dalla libreria un token personalizzato non necessario o inutilizzato. Non è possibile rimuovere i token predefiniti.

Per rimuovere token personalizzati dalla libreria

1. Fare clic sulla scheda Amministrazione, e quindi sulla sottoscheda Raccolta registri.

   Verrà visualizzato l'elenco cartella di Raccolta registri.

2. Fare clic sulla freccia accanto alla cartella Libreria di perfezionamento eventi per espanderla, quindi selezionare la cartella Mapping e Analisi.

   I pulsanti di integrazione del prodotto vengono visualizzati nel riquadro dei dettagli.

3. Fare clic su Nuova regola di analisi del messaggio:

   Viene aperta la procedura guidata file di analisi.

4. Procedere al passaggio Trova corrispondenza e analizza.

5. Selezionare qualsiasi filtro di corrispondenza preliminare e fare clic su Modifica oppure su Aggiungi un filtro di analisi nella parte superiore dell'elenco Filtri di analisi.

   Verrà visualizzata la procedura guidata di analisi filtro file.

6. Proseguire fino al passaggio Espressione regolare.

7. Fare clic su Aggiungi/Rimuovi token dalla libreria

   Verrà visualizzata la finestra di dialogo della libreria dei token di analisi, con visualizzati in nero i token personalizzati e in verde quelli predefiniti.

8. Selezionare uno o più token personalizzati che si desidera rimuovere e fare clic su Rimuovi token selezionato dalla libreria.

   Viene visualizzata una finestra di dialogo di conferma.

9. Fare clic su Sì e quindi su OK.

Importazione di token di analisi

È possibile importare token di analisi per aggiungere al server corrente token di analisi personalizzati creati su un altro server di gestione, ad esempio da un ambiente di prova a un ambiente attivo.

Per importare token di analisi

1. Fare clic sulla scheda Amministrazione, e quindi sulla sottoscheda Raccolta registri.

   Verrà visualizzato l'elenco cartella di Raccolta registri.

2. Fare clic sulla freccia accanto alla cartella Libreria di perfezionamento eventi per espanderla, quindi selezionare la cartella Mapping e Analisi.

   I pulsanti di integrazione del prodotto vengono visualizzati nel riquadro dei dettagli.

3. Fare clic su Nuova regola di analisi del messaggio:

   Viene aperta la procedura guidata file di analisi.

4. Procedere al passaggio Trova corrispondenza e analizza.
5. Selezionare qualsiasi filtro di corrispondenza preliminare e fare clic su Modifica oppure su Aggiungi un filtro di analisi nella parte superiore dell'elenco Filtri di analisi.

   Verrà visualizzata la procedura guidata di analisi filtro file.

6. Proseguire fino al passaggio Espressione regolare.
7. Fare clic su Importa token utente nella parte superiore del riquadro Token di analisi.

   Viene visualizzata la finestra di dialogo Importa file.

8. Individuare il file dei token (.tok) da importare e fare clic su OK.

   Viene visualizzata una finestra di dialogo di conferma.

9. Se si desidera importare il file sovrascrivendo gli altri token della libreria, fare clic su Sì.

Esportazione di token di analisi

È possibile esportare i token di analisi aggiunti dall'utente alla libreria dei token per trasferire su un altro server i token di analisi personalizzati creati sul server di gestione corrente. Ad esempio, è possibile spostare token personalizzati da un ambiente di prova in un ambiente attivo.

Per esportare token di analisi

1. Fare clic sulla scheda Amministrazione, e quindi sulla sottoscheda Raccolta registri.

   Verrà visualizzato l'elenco cartella di Raccolta registri.

2. Fare clic sulla freccia accanto alla cartella Libreria di perfezionamento eventi per espanderla, quindi selezionare la cartella Mapping e Analisi.

   I pulsanti di integrazione del prodotto vengono visualizzati nel riquadro dei dettagli.

3. Fare clic su Nuova regola di analisi del messaggio:

   Viene aperta la procedura guidata file di analisi.

4. Procedere al passaggio Trova corrispondenza e analizza.
5. Selezionare qualsiasi filtro di corrispondenza preliminare e fare clic su Modifica oppure su Aggiungi un filtro di analisi nella parte superiore dell'elenco Filtri di analisi.

   Verrà visualizzata la procedura guidata di analisi filtro file.

6. Proseguire fino al passaggio Espressione regolare.
7. Fare clic su Esporta token utente nella parte superiore del riquadro Token di analisi.

   Viene visualizzata la finestra di dialogo della posizione del download.

8. Scegliere la posizione in cui si desidera salvare il file esportato e fare clic su Salva.

   Il file esportato viene salvato nella posizione scelta.

Analisi del file XMP

È possibile ricorrere all'utility di analisi dei messaggi per analizzare il file nuovo o modificato e determinare l'efficacia del file di analisi a fronte degli eventi campione. L'analisi consente di apportare modifiche per aumentare l'efficienza del file prima di salvarlo.

L'utility analizza un file XMP a fronte dell'evento campione selezionato impostato avvalendosi della seguente procedura:

1. Individuazione di tutti gli eventi contenenti le stringhe di corrispondenza preliminare definite nel file XMP. L'utility avvia una ricerca separata per ogni stringa di corrispondenza preliminare e trova tutti gli eventi che contengono tale stringa.
2. Ricerca del primo filtro di analisi per ognuno degli eventi di corrispondenza preliminare che possono analizzare l'evento in token.

Per analizzare il file XMP

Aprire la procedura guidata file di analisi e avanzare fino al passaggio Analisi. La procedura guidata visualizza il numero di corrispondenze per i filtri e le stringhe di corrispondenza preliminare. Maggiore è il numero di corrispondenze, maggiore sarà l'efficienza del file XMP nuovo o modificato. Questo consente anche di determinare la presenza di informazioni rilevanti che non sono state analizzate.

Nel caso in cui il file XMP e il numero di eventi campione siano grandi, può essere necessario un po' di tempo per l'elaborazione da parte del file XMP. Il processo solitamente non richiede più di un minuto. È possibile annullare questo processo se il tempo impiegato è eccessivo, per poi ripetere l'analisi con un numero di eventi inferiore.

Quando viene creata una nuova regola, essa viene salvata come versione 1.0. Se in seguito la regola viene modificata, una copia separata viene memorizzata come nuova versione. È possibile visualizzare le versioni precedenti e applicarle o copiarle, secondo necessità.

Modalità di creazione di un file di mapping dei dati

È possibile utilizzare la procedura guidata di mapping di file per creare e modificare file di mapping dei dati, che consentono di convertire gli eventi nativi in eventi perfezionati tramite la mappatura delle stringhe di testo analizzate o delle coppie campo/valore a campi compatibili con la CEG. La procedura guidata di mapping di file permette di creare e modificare vari tipi di mapping a questo scopo.

Il processo di creazione o modifica di un file DM comprende i passaggi seguenti:

1. Apertura della procedura guidata di mapping di file.
2. Fornitura dei dettagli del file.
3. Individuazione e aggiunta di eventi campione tramite file di analisi.
4. Impostazione di mapping diretti secondo necessità.
5. Impostazione di mapping diretti secondo necessità.
6. Impostazione di mapping diretti secondo necessità.
7. Impostazione di mapping diretti secondo necessità.

   Nota: è possibile impostare mapping diretti o di funzioni tramite i mapping di blocco. Si tratta di un'alternativa all'impostazione dei mapping con i passaggi 4 e 5.
8. Analisi e salvataggio del file DM completato.

Quando si crea un file DM, occorre considerare le priorità di mapping dei dati del file stesso, oltre ai singoli tipi di mapping all'interno del file. Il file DM completo controlla le informazioni sugli eventi secondo l'ordine delle schermate del tipo di mapping (passaggi 4-7 della procedura guidata). Se esistono tipi di mapping duplicati, l'ultimo valore trovato dal file DM è quello assegnato.

Ad esempio, se un file DM trova un mapping diretto per un dato valore di un evento nativo e poi un mapping condizionale diverso per lo stesso valore, l'evento perfezionato utilizza il risultato del mapping condizionale.

I mapping duplicati *nell'ambito di* un dato tipo di mapping vengono gestiti in modo differente, a seconda del tipo:

- Mapping diretti e di funzione: il file DM utilizza il più recente valore corrispondente trovato. Se viene rilevato un mapping di funzione duplicato, verrà richiamata la funzione più recente. Ad esempio, è possibile impostare un mapping duplicato per richiamare una seconda funzione se la prima non è stata trovata o non ha funzionato come previsto.
- Mapping condizionale e mapping di blocco: il file DM applica il primo valore trovato e termina la ricerca. Per migliorare le prestazioni, occorre stabilire precedentemente nel file più condizioni comuni per entrambi questi tipi di mapping.

Ulteriori informazioni sulle implicazioni di progettazione dell'ordine di mapping sono incluse nelle procedure individuali del tipo di mapping.

Ulteriori informazioni

Impostazione dei mapping di blocco (a pagina 579)
Esecuzione dell'analisi del mapping (a pagina 581)

Apertura della procedura guidata di mapping di file

Per creare un nuovo file DM o modificarne uno esistente, è necessario aprire la procedura guidata di mapping di file.

Per aprire la procedura guidata di mapping di file

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria.
2. Fare clic sulla freccia accanto a alla cartella Integrazione Log per espanderla, quindi selezionare la cartella Mapping e parsing.

   I pulsanti di integrazione del prodotto vengono visualizzati nel riquadro dei dettagli.
3. Fare clic su Nuovo file di mapping:

   Viene visualizzata la procedura guidata di mapping di file.

   Quando si utilizza la procedura guidata:

   - Fare clic su Salva per memorizzare il file senza chiudere la procedura guidata.
   - Fare clic su Salva e chiudi per salvare il file e chiudere la procedura guidata.
   - Fare clic su Reimposta per ripristinare la visualizzazione della procedura guidata alle ultime impostazioni salvate.

Ulteriori informazioni

Impostazione del mapping di funzione di concatenazione (a pagina 576)
Impostazione dei mapping di blocco (a pagina 579)
Esecuzione dell'analisi del mapping (a pagina 581)

Fornire dettagli dei file

Fornisce i dettagli per un nuovo file di DM. È possibile salvare un file di sottoscrizione come personalizzato con un nome diverso.

Per fornire dettagli dei file di mapping

1. Aprire la procedura guidata di mapping di file.
2. Immettere un nome per il file DM. Il nome del file è obbligatorio e non può contenere i caratteri: / \ : * ? “ < > ^;'`,&{}[]. o |.
3. Selezionare il nome del file di analisi e la versione da utilizzare per analizzare gli eventi di esempio dall'elenco a discesa File di analisi.

   Il campo del nome di registro viene riempito automaticamente con il nome del file di analisi inserito.
4. (Facoltativo) Immettere una descrizione.
5. (Facoltativo) Nell'area Informazioni di supporto, fare clic su Aggiungi prodotto per inserire un nome ed una versione di prodotto per scopi di riferimento.
6. Fare clic sulla freccia appropriata per andare al passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Facendo clic su Salva e chiudi, nell'elenco della cartella Utente file di analisi verrà visualizzato il nuovo file; in caso contrario, verrà visualizzato il passaggio scelto dall'utente.

Fornitura degli eventi campione

È possibile utilizzare la procedura guidata di mapping di file per cercare gli eventi campione da utilizzare per l'analisi del file DM. Si può eseguire una ricerca nell'archivio registro eventi o fornire eventi campione direttamente da un file di registro. Gli eventi campione forniscono un modello a fronte del quale verificare l'output di mapping nell'ultimo passaggio della procedura guidata.

Per fornire esempi campione

1. Aprire la procedura guidata di mapping di file e avanzare fino al passaggio Eventi campione.

   Verrà visualizzata la schermata Eventi campione.

2. Nell'area Trova eventi campione, selezionare il pulsante di opzione Archivio di registro o File di registro.
3. Se si seleziona Archivio di registro:
   a. Scegliere il tipo di origine evento campione desiderato dal menu a discesa Colonna di analisi. Selezionare result_string per le origini evento WMI, oppure raw_event per le origini evento syslog.
   b. Utilizzando Filtro tag query ed Elenco query, selezionare la query da utilizzare per fornire eventi campione.

      Verrà visualizzata la query contenente gli eventi campione.

      Nota: è possibile utilizzare tutte le query disponibili o personalizzate per individuare gli eventi campione. Per utilizzare una query personalizzata, è consigliabile crearla e verificarla prima di iniziare il processo di progettazione del file di mapping dati.
4. Se si seleziona File di registro:
   a. Individuare il file di registro desiderato e fare clic su Invia.

      Gli eventi provenienti dal file di registro vengono visualizzati nel pannello Eventi campione.

      Nota: la procedura guidata presume che ogni riga del file sia un evento. Gli eventi su più righe non sono supportati.
   b. Se il file di registro campione contiene valori di coppia dinamici da inserire nel campione analizzato, fare clic su Estrai campi dinamici.
5. Fare clic sulla freccia appropriata per andare al passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Facendo clic su Salva e chiudi, nell'elenco della cartella Utente file di analisi verrà visualizzato il nuovo file; in caso contrario, verrà visualizzato il passaggio scelto dall'utente.

Ulteriori informazioni:

Analisi dinamica (a pagina 559)

Impostazione di mapping diretti

I mapping diretti impostano corrispondenze 1-1 tra un evento nativo e un valore di un singolo evento perfezionato. Pertanto, è meglio utilizzare il mapping diretto solo per i valori predefiniti oppure per i valori comuni che cambiano saltuariamente, ad esempio il campo ideal_model.

È possibile impostare un mapping perché derivi il valore di un evento perfezionato come segue:

Valore testo

Imposta un testo specifico per uno specifico campo CEG. Questo valore viene visualizzato ogni volta che viene mappato un evento appropriato. Ad esempio, l'impostazione del campo CEG ideal_model su "Firewall" ha come risultato la visualizzazione nel campo ideal_model di "Firewall" per tutte le regole che contengono tale mapping.

Valore campo

Imposta un evento non elaborato il cui contenuto è incluso per uno specifico campo CEG o analizzato. Un valore campo si distingue da un valore testo perché preceduto dal simbolo del dollaro, $. Ad esempio, l'impostazione del campo CEG event_logname su "$Registro" ha come risultato la visualizzazione in tutti gli eventi mappati di qualunque testo sia contenuto nel campo Registro dell'evento nativo.

Per impostare i mapping diretti

1. Aprire la procedura guidata del file di mapping, immettere un nome, selezionare un Nome registro per il file di mapping e procedere al passaggio Mapping diretti.

   Viene visualizzata la schermata Mapping diretti, che mostra i mapping correnti o predefiniti. La colonna Nome mostra il nome del campo CEG o analizzato. La colonna Valore mostra un valore testo o un valore campo.

   Nota: è necessario selezionare un file di analisi al passaggio Fornire eventi campione per poter visualizzare i valori dei campi analizzati.

2. Fare clic su Aggiungi mapping diretto per aggiungere una nuova voce di mapping nella parte inferiore della tabella e poi selezionarla, oppure selezionare un mapping diretto corrente da modificare.

   I mapping diretti per il campo, se presenti, vengono visualizzati nell'area Dettagli di mapping.

3. Selezionare dal menu a discesa Campo un campo CEG o un campo evento analizzato, se disponibile, per eseguire il mapping. Durante la digitazione, la funzione auto-complete (auto-completamento) riduce i campi CEG disponibili nell'elenco.
4. Immettere un nuovo valore nel campo Aggiungi valore e fare clic sulla voce Aggiungi mapping diretto accanto ad esso. Far precedere il valore dal carattere "$" per indicare un valore di campo e non un valore di testo.

   Tale valore viene visualizzato nell'area Campi selezionati.
5. (Facoltativo) È possibile immettere più mapping diretti in un singolo campo, utilizzando le frecce su e giù per impostare l'ordine con il quale il file DM li prenderà in considerazione. L'evento perfezionato permette di visualizzare l'ultimo mapping diretto individuato dal file DM.

   Nota: l'aggiunta di valori multipli riduce le prestazioni del mapping, pertanto è opportuno utilizzare questa caratteristica in modo limitato.
6. (Facoltativo) Utilizzare il controllo pilota per spostare i valori non necessari nell'area Campi disponibili. Così facendo, tali valori non saranno presi in considerazione per il mapping corrente.
7. Una volta aggiunti tutti i mapping diretti desiderati, fare clic sulla freccia appropriata per procedere al passaggio relativo alla procedura guidata che si desidera completare, oppure fare clic su Salva e chiudi.

Facendo clic su Salva e chiudi, nella cartella Utente file di mapping verrà visualizzato il nuovo file; in caso contrario, verrà visualizzato il passaggio scelto dall'utente.

Impostazione dei mapping di funzione

I mapping di funzione collegano un campo CEG ad un valore utilizzando una funzione per recuperare o definire le informazioni dell'evento perfezionato che vengono visualizzate nell'evento perfezionato. Tutti i mapping di funzione sono composti da un nome di campo CEG, da un valore di campo predefinito o di classe e dalla funzione.

Ad esempio, un mapping di funzione potrebbe concatenare una serie di valori di eventi nativi in un singolo campo CEG, utilizzando la funzione di concatenazione.

In caso di mapping di funzione duplicati, il file DM utilizzerà l'ultimo mapping trovato. È possibile impostare un mapping duplicato per richiamare una seconda funzione, se la prima non è stata trovata o non ha funzionato come previsto.

Per impostare i mapping di funzione

1. Aprire la procedura guidata dei file di mapping, inserire un nome e selezionare un Nome registro per il file di mapping. Fatto ciò, avanzare al passaggio Mapping di funzione.

   Viene visualizzata la schermata Mapping di funzione, che mostra i mapping correnti o predefiniti. La colonna Nome contiene un campo CEG o analizzato, mentre la colonna Funzione contiene la funzione di collegamento corrente. La colonna Valore contiene invece un valore di testo o di campo.

   Nota: per visualizzare i valori di campo analizzati, selezionare un file di analisi al passaggio Fornire i dettagli del file.

2. Fare clic su Aggiungi mapping di funzione per aggiungere una nuova voce di mapping, oppure selezionare un mapping corrente da modificare.

   La voce di mapping viene visualizzata nel pannello Dettagli di mapping.

3. Dal menu a discesa Campo, deselezionare un campo CEG da mappare. Quando si inizia a digitare, la funzione di completamento automatico restringerà l'elenco dei campi CEG disponibili.

4. Selezionare una funzione da utilizzare per il mapping dal menu a discesa Funzione.

   Nota: la funzione di concatenamento (concat) funziona in maniera differente dalle altre, poiché consente di specificare più valori di destinazione. Per ulteriori informazioni, vedere Impostare il mapping di una funzione di concatenamento.

5. Inserire un valore di destinazione per il mapping nel campo Aggiungi valore e fare clic sul pulsante Aggiungi valore accanto ad esso. Far precedere il valore dal carattere "$" per indicare un valore di campo e non un valore specifico.

   Tale valore viene visualizzato nell'area Campi selezionati.

6. (Facoltativo) È possibile inserire mapping multipli per un singolo campo. A tale scopo, utilizzare le frecce verso l'alto e verso il basso per impostare l'ordine di considerazione dei mapping da parte del file di DM.

   Nota: aggiungendo più valori diminuiranno le prestazioni del mapping, pertanto si consiglia di utilizzare i mapping di funzione stand-alone solo se necessario.

7. (Facoltativo) Utilizzare il controllo pilota per spostare i valori non necessari nell'area Campi disponibili. Così facendo, tali valori non saranno presi in considerazione per il mapping corrente.
8. Dopo aver aggiunto tutti i mapping di funzione desiderati, fare clic sulla freccia appropriata per avanzare al passaggio della procedura guidata da completare, oppure fare clic su Salva e chiudi.

   Facendo clic su Salva e chiudi, nell'elenco della cartella Utente file di analisi verrà visualizzato il nuovo file; in caso contrario, verrà visualizzato il passaggio scelto dall'utente.

Impostazione del mapping di funzione di concatenazione

Il mapping di una funzione di concatenazione è un tipo di mapping di funzione. A differenza degli altri mapping di funzione, che specificano un solo campo o valore di destinazione, la funzione di concatenazione specifica più destinazioni di mapping, che concatena poi in un solo campo CEG.

È possibile utilizzare la procedura guidata di mapping di dati per creare mapping di funzioni concatenate. Dato che i mapping di concatenazione sono diversi dagli altri mapping di funzione, anche la procedura per crearli è un po' differente.

Per impostare il mapping di funzione di concatenazione

1. Aprire la procedura guidata di mapping di file, specificare un nome e selezionare un nome registro per il file di mapping; quindi, procedere con il passaggio Mapping di funzione.

   Viene visualizzata la schermata Mapping di funzione, che mostra i mapping correnti o predefiniti. La colonna Nome mostra un campo CEG, la colonna Funzione visualizza la funzione di collegamento corrente, mentre nella colonna Valore appare un valore testo o campo.
2. Fare clic su Aggiungi mapping di funzione per aggiungere una nuova voce di mapping

   La voce di mapping viene visualizzata nel pannello Dettagli di mapping.
3. Selezionare dal menu a discesa Campo un campo CEG per eseguire il mapping.

4. Selezionare la funzione di concatenazione dal menu a discesa Funzione.

   Vengono visualizzati i campi Formato e Valore.

   Nota: il valore della funzione di concatenazione viene visualizzato come {...} nel pannello Mapping di funzione. Questo significa che è presente un set di valori anziché un solo valore.

5. (Facoltativo) Inserire un identificatore nel campo Formato per controllare l'inserimento dei campi di destinazione. L'indicatore di formato, %s, indica una posizione nel campo. Qualsiasi elemento diverso da %s viene considerato come dati di supporto statici da includere nel campo di raccolta della tabella finale. Ad esempio, per separare due campi di destinazione con due punti, inserire "%s:%s" nel campo Formato.

6. Fare clic su Aggiungi valore di concatenazione nell'area Valori di concatenazione per aggiungere una coppia input-valore di destinazione.

7. Inserire un valore nel campo di immissione Aggiungi valore e fare clic sul pulsante omonimo.

   Tale valore viene visualizzato nell'area Campi selezionati.

8. Ripetere i passaggi 6 e 7 per inserire valori aggiuntivi da concatenare. Occorre aggiungere almeno due valori di destinazione.

9. Una volta aggiunti tutti i mapping di concatenazione desiderati, fare clic sulla freccia appropriata per andare al passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, il nuovo file viene visualizzato nella cartella Utente file di analisi; altrimenti, verrà visualizzato il passaggio selezionato.

Impostazione dei mapping condizionali

I mapping condizionali collegano un campo CEG a diversi risultati possibili, consentendo di impostare valori predefiniti e condizionali per un dato campo. Ad esempio, è possibile utilizzare i mapping condizionali per mappare i valori di riuscita o non riuscita, oppure per identificare le origini evento in base al nome o al gruppo.

Il mapping condizionale assegna un valore predefinito ed uno o più valori condizionali ad un dato campo CEG. È possibile impostare le qualifiche per ogni valore condizionale. Se un evento corrisponde a queste qualifiche, il valore condizionale appropriato verrà assegnato al campo selezionato. In caso contrario, l'evento perfezionato mostrerà il valore predefinito.

In caso di mapping condizionali duplicati, il file di DM utilizzerà il primo mapping trovato e non prenderà in considerazione nessun altro mapping. Per prestazioni migliori, occorre prima stabilire più condizioni comuni.

Nota: il mapping condizionale indipendente è più lento di quello a blocchi. Utilizzarlo solo se strettamente necessario.

Per impostare i mapping condizionali

1. Aprire la procedura guidata relativa ai file di mapping, inserire un nome e selezionare un Nome di registro per il file di mapping. Fatto ciò, proseguire al passaggio Mapping condizionali.

   Viene visualizzata la schermata Mapping condizionale, che mostra tutti gli eventuali mapping predefiniti correnti. La colonna Campo contiene il nome del campo CEG o analizzato, mentre la colonna Valore contiene il valore corrente predefinito.

   Nota: per visualizzare i valori di campo analizzati, selezionare un file di analisi nel passaggio Fornire i dettagli del file.

2. Fare clic su Aggiungi mapping condizionale nell'elenco Mapping campo condizionale e selezionare la nuova riga.

   Verrà visualizzato il riquadro Dettagli di mapping, contenente l'elenco a discesa Campo ed il controllo pilota Valore.

3. Nel menu Campo, selezionare il campo CEG da mappare. Quando si inizia a digitare, la funzione di completamento automatico restringerà l'elenco dei campi CEG disponibili.

4. Inserire il mapping predefinito nel campo Aggiungi valore e fare clic su Aggiungi valore per visualizzarlo nel riquadro Campi selezionati. È possibile eliminare i valori indesiderati spostandoli nel riquadro Campi disponibili.

5. Fare clic su Aggiungi valore condizionale nell'elenco Valori condizionali.

   Viene visualizzato un nuovo valore.

6. Selezionare il testo Nuovo valore per evidenziarlo e modificare il nome.

   Il nuovo nome verrà visualizzato nell'elenco e la finestra dei filtri verrà visualizzata nel riquadro dei dettagli.

7. Creare un filtro per definire il valore condizionale. Ad esempio, è possibile creare uno o più filtri per collegare il campo event_source_address agli indirizzi IP, identificando l'origine evento con un gruppo geografico o un altro gruppo di business.
8. Una volta aggiunti tutti i mapping condizionali desiderati, fare clic sulla freccia appropriata per avanzare al passaggio della procedura guidata da completare, oppure fare clic su Salva e chiudi.

   Facendo clic su Salva e chiudi, nell'elenco della cartella Utente file di analisi verrà visualizzato il nuovo file; in caso contrario, verrà visualizzato il passaggio scelto dall'utente.

Impostazione dei mapping di blocco

I mapping di blocco collegano una condizione selezionata a una serie definita di mapping, consentendo di creare una sovrapposizione di mapping attivata da tale condizione. Un determinato mapping di blocco può utilizzare una qualunque combinazione di mapping diretti o di funzione. Entrambi i tipi di mapping di blocco interni funzionano esattamente come i mapping stand-alone.

È possibile creare tanti blocchi quanti ne occorrono per un singolo file di mapping. Ognuno di essi include un nome e una condizione.

Se in un determinato blocco sono presenti mapping duplicati, il file DM sfrutterà il primo che trova e non considererà ulteriori mapping. Per migliorare la performance, occorre prima stabilire più condizioni comuni.

Per impostare i mapping di blocco

1. Aprire la procedura guidata di mapping di file, specificare un nome e selezionare un nome registro per il file di mapping; quindi, procedere con il passaggio Mapping diretti.

   Viene visualizzata la schermata Mapping di blocco, che mostra tutti i mapping di blocco correnti.
2. Fare clic su Aggiungi mapping di blocco nel pannello Mapping di blocco.

   Nell'elenco Mapping di blocco viene visualizzato un nuovo blocco.

3. Selezionare il testo del nuovo blocco.

   Viene visualizzato il pannello Definizione blocco, che mostra il passaggio 1. Definizione di una condizione

4. Inserire un nome blocco e creare un filtro che ne definisca la condizione. Ad esempio, è possibile definire event_result come equivalente a "S", in modo da richiamare i mapping di blocco quando l'elaborazione dell'evento viene completata con successo.

5. Fare clic sulla barra del passaggio 2 e inserire tutti i mapping diretti desiderati, con lo stesso procedimento utilizzato per il mapping stand-alone.

6. Fare clic sulla barra del passaggio 3 e inserire tutti i mapping di funzione desiderati, con lo stesso procedimento utilizzato per il mapping stand-alone.

7. Una volta aggiunti tutti i mapping di blocco desiderati, fare clic sulla freccia appropriata per andare al passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, il nuovo file viene visualizzato nella cartella Utente file di analisi; altrimenti, verrà visualizzato il passaggio selezionato.

Ulteriori informazioni

Utilizzo di filtri avanzati (a pagina 584)

Esecuzione dell'analisi del mapping

È possibile utilizzare la procedura guidata di mapping per analizzare un file di mapping di dati, in modo da poter eseguire verifiche e modifiche per aumentare l'efficienza del proprio file DM. Gli eventi campione vengono verificati a fronte del file DM e i risultati vengono poi convalidati a fronte della CEG.

Per eseguire l'analisi, fare clic sul passaggio Analisi del mapping della procedura guidata di mapping di file. La procedura permette di visualizzare una tabella che mostra i risultati degli eventi campione inseriti nel passaggio Evento campione.

Il file DM completato salva i mapping e considera le informazioni sugli eventi nell'ordine delle schermate relative al tipo di mapping (passaggi 4-7 della procedura guidata). Se esistono mapping duplicati, l'ultimo valore trovato dal file DM è quello che viene assegnato. Ad esempio, se un file DM trova un mapping diretto per un determinato valore di un evento nativo e successivamente un mapping condizionale diverso per lo stesso valore, l'evento perfezionato mostra il risultato del mapping condizionale. Ulteriori informazioni sulle implicazioni di progettazione dell'ordine di mapping sono incluse nelle procedure individuali del tipo di mapping.

Quando viene creata una nuova regola, essa viene salvata come versione 1.0. Se in seguito la regola viene modificata, una copia separata di essa viene memorizzata come nuova versione. È possibile visualizzare le versioni precedenti e applicarle o copiarle, secondo necessità.

Attività delle regole di inoltro eventi

Le regole di inoltro eventi consentono di selezionare gli eventi di CA User Activity Reporting Module da inviare ai listener remoti di sistemi o applicazioni esterni. È possibile utilizzare regole di inoltro per identificare gli eventi da inoltrare, per impostare il momento in cui verranno trasmessi e per controllare il modo in cui verranno ricevuti. Se un evento in arrivo corrisponde al filtro di una regola di inoltro, in CA User Activity Reporting Module verrà creata e successivamente inoltrata una copia dell'evento. L'evento è ancora registrato nell'archivio registro eventi.

L'area Raccolta registri dell'interfaccia di CA User Activity Reporting Module consente di gestire le attività delle regole di inoltro eventi. È possibile creare, modificare ed eliminare le regole di inoltro eventi. È inoltre possibile importare o esportare le regole di inoltro eventi.

Ulteriori informazioni:

Come creare regole di inoltro eventi. (a pagina 582)

Come creare regole di inoltro eventi.

È possibile utilizzare regole di inoltro eventi per inviare eventi di CA User Activity Reporting Module ad applicazioni esterne. Ad esempio, utilizzando syslog è possibile inviare eventi a CA NSM. Le regole di inoltro eventi consentono di impostare i criteri per gli eventi da inoltrare, ed impostare uno o più ricevitori.

Il processo di creazione delle regole di inoltro eventi con la relativa procedura guidata è composto dai seguenti passaggi:

1. Aprire la procedura guidata delle regole di inoltro.
2. Definire un nome ed una descrizione facoltativa per la regola.
3. Creare filtri semplici ed avanzati per identificare gli eventi da inoltrare.
4. Definire attributi di regola che comprendono la destinazione di inoltro ed i campi CEG da inserire nell'evento inoltrato.

Ulteriori informazioni:

Nome della regola di inoltro (a pagina 583)
Creazione di un filtro evento semplice (a pagina 584)
Creazione di un filtro di eventi avanzato (a pagina 586)
Utilizzo di filtri avanzati (a pagina 524)
Impostare gli attributi della regola di inoltro (a pagina 587)

Aprire la procedura guidata delle regole di inoltro

Per creare una nuova regola di inoltro o modificarne una esistente, aprire la relativa procedura guidata.

Per aprire la procedura guidata delle regole di inoltro

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria.
2. Selezionare la cartella Regole di inoltro.

   I pulsanti della regola di inoltro vengono visualizzati nel riquadro dei dettagli.
3. Fare clic su Nuova regola di inoltro:

   Verrà visualizzata la procedura guidata delle regole di inoltro.

   Quando si utilizza la procedura guidata:

   - Fare clic su Salva per salvare il file della regola senza chiudere la procedura guidata.
   - Fare clic su Salva e chiudi per salvare il file della regola e chiudere la procedura guidata.
   - Fare clic su Reimposta per ripristinare la visualizzazione della procedura guidata alle ultime impostazioni salvate.

Nome della regola di inoltro

Assegnare un nome ad una regola di inoltro. È anche possibile immettere informazioni descrittive da usare come riferimento.

Per assegnare un nome ad una regola di inoltro

1. Aprire la procedura guidata delle regole di inoltro.
2. Immettere un nome per la nuova regola. Il nome del file è obbligatorio e non può contenere i caratteri: / \ : * ? < >;'`,&{}[]. o |.
3. (Facoltativo) Inserire informazioni descrittive relative alla regola a scopo di riferimento.
4. Procedere al passaggio Filtraggio.

Creazione di un filtro evento semplice

È possibile creare filtri semplici per definire parametri di ricerca per i campi comuni CEG. Ad esempio, si potrebbe impostare il campo Modello ideale su "Amministrazione contenuti" per identificare tutti gli eventi con quel valore nel campo CEG Modello ideale. I filtri semplici vengono utilizzati da molte funzionalità, incluse le query, le regole di soppressione e riepilogo e le regole di inoltro degli eventi.

Per creare un filtro semplice

1. Selezionare la casella di controllo Modello ideale o uno dei campi Evento che si desidera definire, quindi selezionare un valore nell'elenco a discesa oppure immettere il valore desiderato nel campo di immissione del testo.
2. (Facoltativo) Se si crea un filtro query, selezionare una delle caselle di controllo dei campi Origine, Destinazione o Agente e immettere il valore desiderato nel campo di immissione del testo.
3. Per aggiungere altri filtri semplici, ripetere i passaggi da 1 a 2.
4. Dopo aver aggiunto tutti i filtri semplici desiderati, fare clic su Salva.

Ulteriori informazioni

Utilizzo di filtri avanzati (a pagina 584)
Creazione di un filtro di eventi avanzato (a pagina 586)

Utilizzo di filtri avanzati

È possibile utilizzare filtri avanzati basati su SQL per definire le funzioni che interrogano l'archivio registro eventi, come il perfezionamento delle query o la personalizzazione di filtri rapidi. L'interfaccia Filtri avanzati consente di creare la sintassi dei filtri appropriata mediante un modulo in cui è possibile immettere colonne, operatori e valori logici in base ai requisiti di filtro.

Nota: nella presente sezione è contenuta una breve descrizione dei termini SQL utilizzati nei filtri avanzati. Per sfruttare al massimo i filtri avanzati, occorre una conoscenza approfondita di SQL e della Common Event Grammar.

I seguenti termini SQL si associano a più istruzioni del filtro:

And

Consente di visualizzare le informazioni sugli eventi se *tutti* i termini associati risultano veri.

Or

Consente di visualizzare le informazioni sugli eventi se *uno* dei termini associati risulta vero.

Having

Perfeziona i termini dell'istruzione SQL principale aggiungendo un'istruzione qualificante. Ad esempio, è possibile impostare filtri avanzati per eventi da host specifici e aggiungere un'istruzione "having" per restituire da quegli host soltanto eventi di un livello di gravità specifico.

I seguenti operatori SQL vengono utilizzati dai filtri avanzati per creare le condizioni di base:

Operatori relazionali

Comprendono le informazioni sugli eventi se sussiste la relazione appropriata tra la colonna e il valore immesso. Sono disponibili i seguenti operatori relazionali:

- Pari a
- Diverso da
- Minore di
- Maggiore di
- Minore o uguale a
- Maggiore o uguale a

Ad esempio, l'operatore *Maggiore di* include le informazioni sugli eventi dalla colonna selezionata se il relativo valore è maggiore del valore impostato.

Come

Include le informazioni sugli eventi se la colonna contiene uno schema immesso, utilizzando % per impostare lo schema desiderato. Ad esempio, L% restituisce eventuali valori che iniziano con L, %L% restituisce eventuali valori in cui L rappresenta la prima o l'ultima lettera.

Non uguale

Include le informazioni sugli eventi se la colonna non contiene lo schema specificato.

Nel set

Include informazioni sull'evento se la colonna contiene uno o più dei valori nel set racchiuso tra virgolette che è stato specificato. Se nel set sono presenti più valori, essi devono essere separati da virgole.

Non nel set

Include informazioni sull'evento se la colonna non contiene uno più dei valori nel set racchiuso tra virgolette che è stato specificato. Se nel set sono presenti più valori, essi devono essere separati da virgole.

Corrispondenze

Include informazioni sugli eventi corrispondenti a uno o più dei caratteri immessi, in modo da poter condurre ricerche di parole chiave.

Con chiave

Include informazioni sugli eventi impostate come valori chiave durante la configurazione del server di rapporto. È possibile utilizzare valori chiave per impostare la rilevanza per l'azienda o altri gruppi organizzativi.

Senza chiave

Include informazioni sugli eventi non impostate come valori chiave durante la configurazione del Server di rapporto. È possibile utilizzare valori chiave per impostare la rilevanza per l'azienda o altri gruppi organizzativi.

Creazione di un filtro di eventi avanzato

I filtri avanzati vengono utilizzati da molte funzioni, tra cui la creazione di query, la pianificazione di rapporti e i filtri locali e globali.

Per creare un filtro avanzato

1. Fare clic su Nuovo filtro evento.

   La prima riga della tabella dei filtri degli eventi diventa attiva e nelle relative colonne Logico e Operatore vengono visualizzati, rispettivamente, i valori predefiniti "And" e "Equal to".

2. (Facoltativo) Fare clic sulla cella Logico e modificare il valore logico secondo necessità.

3. Fare clic sulla cella Colonna, quindi selezionare la colonna relativa alle informazioni sugli eventi desiderata dal menu a discesa.

4. Fare clic sulla cella Operatore, quindi selezionare l'operatore desiderato dal menu a discesa.

5. Fare doppio clic sulla cella Valore, quindi immettere il valore desiderato.
6. (Facoltativo) Fare clic sulle celle relative alle parentesi aperte e chiuse, quindi immettere il numero di parentesi necessarie.
7. (Facoltativo) Ripetere i passaggi da 1 a 6 secondo necessità per aggiungere ulteriori istruzioni dei filtri.
8. Una volta immesse le istruzioni dei filtri desiderate, fare clic su Salva.

Ulteriori informazioni

Utilizzo di filtri avanzati (a pagina 584)

Impostare gli attributi della regola di inoltro

Impostare gli attributi necessari per una regola di inoltro, come i punti di uscita dell'inoltro, i campi CEG inclusi nell'evento inoltrato e le impostazioni di destinazione.

Per impostare gli attributi della regola

1. Aprire la procedura guidata delle regole di inoltro e accedere al passaggio Attributi di criterio.
2. Nell'area Azioni, impostare le azioni della regola di inoltro:
   a. Selezionare una struttura ed una gravità syslog negli elenchi a discesa appropriati. Qualsiasi evento inoltrato dalla regola comprenderà gli attributi syslog impostati dall'utente.
3. Nell'area Informazioni generali, impostare le informazioni sulla trasmissione degli elenchi di CA User Activity Reporting Module:
   a. Selezionare se gli eventi identificati dalla regola verranno inviati prima o dopo la soppressione ed il riepilogo:
   - Selezionando l'invio degli eventi prima della soppressione e del riepilogo, tutti gli eventi in arrivo verranno verificati con i filtri della regola di inoltro.
   - Selezionando l'invio degli eventi dopo la soppressione e il riepilogo, solo gli eventi perfezionati verranno verificati con i filtri della regola di inoltro. Gli eventi soppressi non verranno inoltrati e quelli riepilogati verranno inoltrati solo in forma di riepilogo e non nei dettagli di preriepilogo.

     Nota: la scelta di inviare gli eventi prima della soppressione e del riepilogo avrà un effetto maggiore sulle prestazioni del sistema, poiché gli eventi non saranno perfezionati.

a. Selezionare i campi CEG da visualizzare nell'evento trasmesso. Se non si seleziona un campo CEG, verrà inviato solo il valore dell'evento non elaborato. Se si seleziona un *qualsiasi* campo CEG, selezionare anche raw_event per inoltrare l'evento non elaborato.

4. Nell'area Destinazione, impostare le informazioni sulla destinazione dell'inoltro.

   a. Per creare una riga di destinazione, fare clic su Aggiungi destinazione.

   b. Fare clic sul testo della colonna Host per aggiungere un nome di host di destinazione o un indirizzo IP. L'indirizzo IP può essere IPv4 o IPv6.

   c. Fare clic sulla cella della colonna Porta per aggiungere il numero di porta su cui l'applicazione di destinazione è in ascolto.

   d. Fare clic sul testo della colonna Protocollo per selezionare TCP o UDP come protocollo di trasmissione da utilizzare.

   e. Ripetere i passaggi a-d per aggiungere ulteriori destinazioni.

5. Fare clic su Salva o su Salva e chiudi.

   La nuova regola verrà visualizzata nella sottocartella Utente della cartella Regole di inoltro.

Informazioni sugli Eventi syslog inoltrati

La dimensione massima del pacchetto syslog (inclusi i campi relativi a PRI, Intestazione, Tag e Contenuto) è pari a 1024 byte. L'evento inoltrato, pertanto, potrebbe non riuscire ad includere tutte le coppie nome-valore CEG specificate dall'utente.

Se necessario, CA User Activity Reporting Module consente di troncare il valore del messaggio per mantenere la lunghezza al di sotto dei 1024 byte. Se la regola di inoltro consente di specificare i campi CEG da includere nell'evento syslog generato, il campo Contenuto di questo evento sysolg comprenderà le coppie nome-valore CEG specificate.

Le coppie nome-valore presentano il formato *CEG_field_name*:*field_value* dell'evento corrispondente alla regola del filtro semplice. La stringa “null” indica un valore nullo del campo CEG. I campi CEG vengono presentati nell'ordine specificato nella regola di inoltro.

L'ordine del campo CEG specificato nella regola di inoltro è significativo. CA User Activity Reporting Module consente di troncare la parte di valore specificata ma non di troncare i nomi di campo CEG. Se a CA User Activity Reporting Module non è consentita l'impostazione del successivo nome di campo CEG completo, dei due punti e di almeno un byte del valore associato, il campo del contenuto di syslog verrà fatto terminare con la coppia nome-valore CEG precedente.

Modifica di una regola di inoltro

È possibile modificare una regola di inoltro.

Per modificare una regola di inoltro

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria.
2. Espandere la cartella Regole di inoltro e fare clic sulla cartella che contiene il file che si desidera modificare.
3. Selezionare la regola da modificare e fare clic sull'icona Modifica regola di inoltro.

   Verrà visualizzata la procedura guidata regola di inoltro con la regola selezionata.
4. Modificare la regola desiderata e fare clic su Salva e chiudi.

   La regola verrà visualizzata nell'elenco appropriato come nuova versione della regola modificata.

Eliminazione di una regola di inoltro

È possibile eliminare un regola di inoltro non necessaria.

Per eliminare una regola di inoltro

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria.
2. Espandere la cartella Regole di inoltro e fare clic sulla cartella che contiene il file che si desidera eliminare.
3. Selezionare la regola da eliminare e fare clic sull'icona Elimina regola di inoltro. La versione corrente è selezionata per impostazione predefinita. È possibile selezionare una versione precedente da eliminare dall'elenco a discesa Versione nel riquadro dei dettagli.

   Viene visualizzata una finestra di conferma.
4. Fare clic su Sì.

   La regola eliminata viene rimossa dall'elenco appropriato.

Importazione di una regola di inoltro

L'importazione di una regola di inoltro consente di trasferire le regole da un ambiente all'altro. Ad esempio, è possibile importare in un ambiente attivo le regole create in un ambiente di prova.

Per importare una regola di inoltro

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria.
2. Selezionare la cartella Regole di inoltro.

   I pulsanti della regola di inoltro vengono visualizzati nel riquadro dei dettagli.
3. Fare clic su Importa regola di inoltro.

   Verrà visualizzata la finestra di dialogo Importa file.
4. Individuare la regola da importare e fare clic su OK.

   Verrà visualizzata la procedura guidata regola di inoltro contenente i dettagli della regola selezionata.
5. Modificare la regola desiderata e fare clic su Salva e chiudi. Se la regola importata ha lo stesso nome di una che si trova già nel database di gestione, verrà richiesto di modificare il nome.

   La regola importata verrà visualizzata nella cartella utente Regole di inoltro eventi.

Esportazione di una regola di inoltro

L'esportazione di una regola di inoltro consente di trasferire le regole da un ambiente all'altro. Ad esempio, è possibile esportare in un ambiente attivo le regole create in un ambiente di prova.

Per esportare una regola di inoltro

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria.
2. Espandere la cartella Regole di inoltro e fare clic sulla cartella che contiene il file che si desidera esportare.
3. Selezionare la regola da esportare e fare clic su Esporta regola di inoltro. La versione corrente è selezionata per impostazione predefinita. È possibile selezionare una versione precedente da esportare dall'elenco a discesa Versione situato nel riquadro dei dettagli.

   Verrà visualizzata la finestra di dialogo relativa alla posizione dell'esportazione.
4. Digitare o accedere al percorso in cui memorizzare la regola esportata e fare clic su Salva.

   Verrà visualizzata una finestra di conferma dell'avvenuta esportazione.
5. Fare clic su OK.

   La regola viene esportata.

   Nota: se si analizza la regola esportata, i valori di Funzionalità e Gravità vengono visualizzati solo in formato numerico. È possibile utilizzare l'interfaccia della procedura guidata per determinare le descrizioni testuali correlate a questi valori.

Capitolo 16: Integrazioni e connettori

Questa sezione contiene i seguenti argomenti:

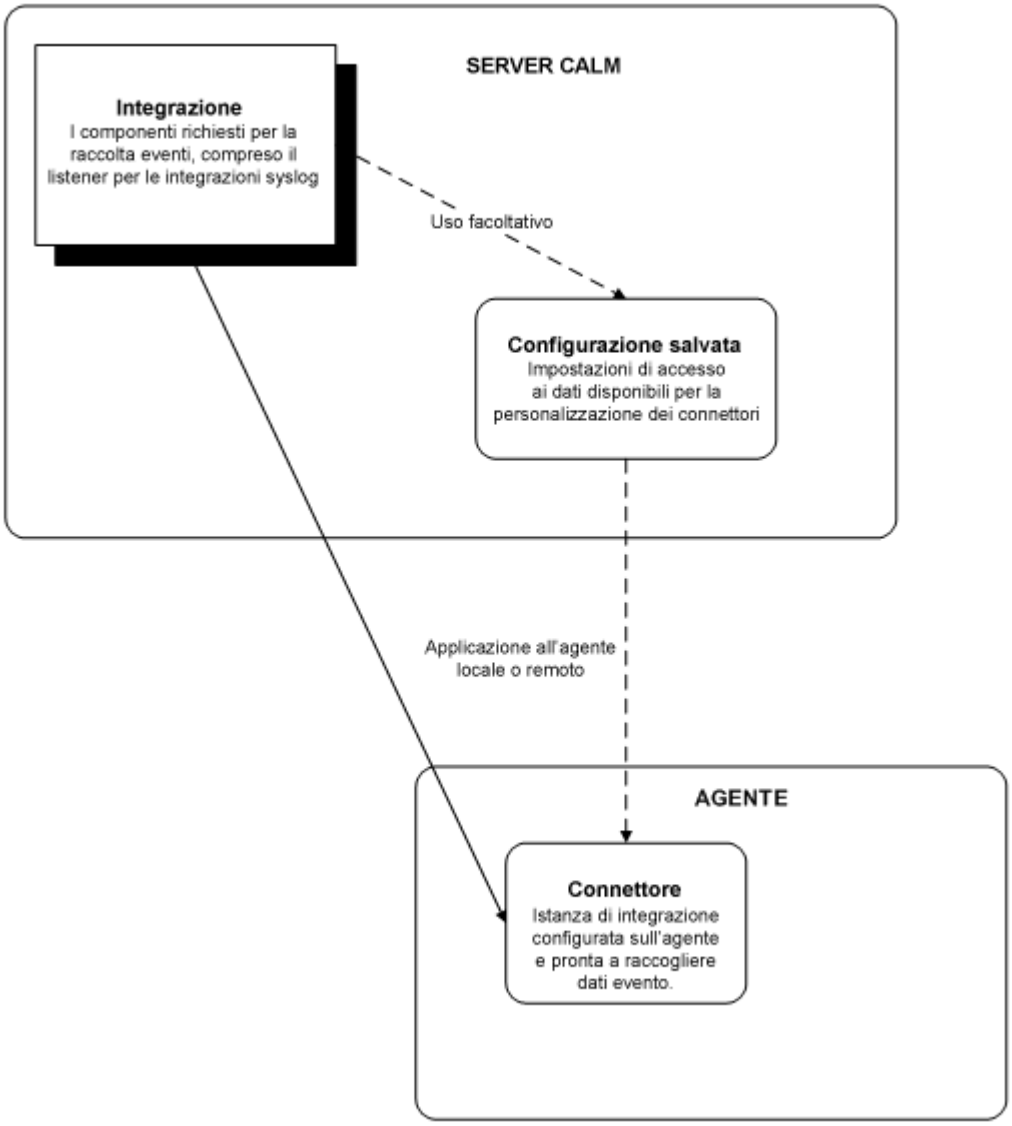
Attività relative a integrazioni e connettori (a pagina 593)
Modalità di creazione di un'integrazione (a pagina 595)
Modalità di creazione di un listener syslog (a pagina 602)
Creazione di una nuova versione di integrazione (a pagina 609)
Eliminazione di un'integrazione (a pagina 610)
Esportazione e importazione delle definizioni delle integrazioni (a pagina 610)
Modalità di creazione di un connettore (a pagina 612)
Visualizzazione di un connettore (a pagina 617)
Visualizzazione di una guida per il connettore (a pagina 617)
Modifica di un connettore (a pagina 618)
Informazioni sulle configurazioni salvate (a pagina 619)
Creazione di una configurazione salvata (a pagina 620)
Come configurare i connettori in blocco (a pagina 621)
Aggiornamento delle configurazioni di più connettori (a pagina 627)

Attività relative a integrazioni e connettori

L'integrazione è un modello per i connettori. Include tutti i componenti necessari alla raccolta di informazioni sugli eventi da un tipo di risorsa specifico: un sensore di registro, file XMP e DM e regole di soppressione facoltative. Le integrazioni vengono fornite da CA. Anche gli utenti possono creare le proprie integrazioni.

È possibile creare un'integrazione personalizzata o modificare la copia di una predefinita. Si possono anche creare i propri file XMP o DM da utilizzare nelle integrazioni personalizzate, oltre a integrazioni salvate contenenti specifiche informazioni di accesso ai dati.

Dopo aver analizzato un evento e creato l'integrazione richiesta, è possibile creare un connettore utilizzando le configurazioni salvate e applicarlo a un agente, come mostrato nell'illustrazione seguente:



Ulteriori informazioni

Esportazione e importazione delle definizioni delle integrazioni (a pagina 610)
Informazioni sulle configurazioni salvate (a pagina 619)
Visualizzazione di un connettore (a pagina 617)
Modifica di un connettore (a pagina 618)

Modalità di creazione di un'integrazione

È possibile utilizzare la procedura guidata di integrazione per creare o modificare le integrazioni, che servono da modelli per i connettori configurati che raccolgono o ricevono eventi dal proprio ambiente.

Si possono creare informazioni di diversi tipi, tra cui integrazioni WMI e ODBC, che raccolgono attivamente eventi del tipo specificato. È anche possibile creare integrazioni syslog che ricevono passivamente gli eventi. Le integrazioni syslog possono ricevere eventi da più origini. Perciò il processo di creazione di un'integrazione syslog e quello di un connettore è leggermente diverso.

Per sfruttare al massimo questa funzione avanzata è necessaria una conoscenza approfondita delle origini evento del proprio ambiente e dei relativi tipi di comunicazione. Inoltre, è necessaria una conoscenza approfondita della normale sintassi di espressione, della CEG, dei file DM e XMP e del modo in cui analizzano gli eventi.

La creazione di un'integrazione include i passaggi seguenti:

1. Apertura della procedura guidata di integrazione.
2. Aggiunta dei componenti dell'integrazione.
3. Selezione delle regole di soppressione.
4. Selezione delle regole di riepilogo.
5. Impostazione delle configurazioni predefinite. Questo passaggio non riguarda le integrazioni syslog.

Si può anche creare un'integrazione utente personalizzata copiando un'integrazione di sottoscrizione.

Ulteriori informazioni:

Aggiunta di componenti dell'integrazione (a pagina 597)
Applicare le regole di soppressione e riepilogo (a pagina 598)
Impostazione delle configurazioni predefinite (a pagina 599)

Apertura della procedura guidata di integrazione

Per creare una nuova integrazione o modificarne una esistente, aprire la procedura guidata di integrazione.

Per aprire la procedura guidata di integrazione

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria.
2. Fare clic sulla freccia accanto alla cartella Integrazione Log per espanderla, quindi selezionare la cartella Integrazioni.

   I pulsanti di integrazione vengono visualizzati nel riquadro dei dettagli.
3. Fare clic su Nuova integrazione:

   Viene visualizzata la procedura guidata di integrazione.

   Quando si utilizza la procedura guidata:

   - Fare clic su Salva per memorizzare il file senza chiudere la procedura guidata.
   - Fare clic su Salva e chiudi per salvare il file e chiudere la procedura guidata.
   - Fare clic su Reimposta per ripristinare la visualizzazione della procedura guidata alle ultime impostazioni salvate.

Ulteriori informazioni:

Aggiunta di componenti dell'integrazione (a pagina 597)

Aggiunta di componenti dell'integrazione

Quando si crea un'integrazione, vengono impostati i principali dettagli di integrazione, come ad esempio i sensori di registro ed i file XMP e DM utilizzati per raccogliere gli eventi.

Per aggiungere componenti dell'integrazione

1. Aprire la procedura guidata di integrazione.
2. Immettere un nome per la nuova integrazione.
3. Selezionare dall'elenco i seguenti componenti obbligatori dell'integrazione:

   Sensore

   Indica il sensore di registro utilizzato dall'integrazione per leggere gli eventi dall'origine del registro.

   Assistente di configurazione

   Indica il file binario dell'assistente utilizzato dall'integrazione per connettersi all'archivio di registro selezionato. Molte integrazioni non richiedono un assistente di configurazione.

   Piattaforma

   Fa riferimento al sistema operativo su cui può essere eseguito cui l'agente di integrazione e *non* al sistema operativo dell'applicazione che l'integrazione è progettata per monitorare. La procedura guidata selezionerà automaticamente il sistema operativo in base alle impostazioni di sensore e configurazione.
4. Inserire una descrizione per l'integrazione.
5. Selezionare con il controllo pilota i file XMP e DM che l'integrazione utilizzerà per perfezionare gli eventi.
6. Se necessario, nel campo Campi di destinazione, digitare il nome del campo nativo contenente le informazioni di evento non elaborato da far analizzare all'integrazione. Alcuni tipi di evento contengono informazioni sugli eventi non elaborati ad essi relativi. Esse risiedono in un campo particolare, al quale è destinata l'integrazione. Ad esempio, per gli eventi del registro eventi NT, tale campo è "Messaggio".
7. Fare clic sulla freccia appropriata per andare al passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, nell'elenco della cartella utente verrà visualizzata la nuova integrazione, oppure il passaggio scelto dall'utente.

Applicare le regole di soppressione e riepilogo

Per semplificare il perfezionamento degli eventi è possibile applicare ad un'integrazione sia regole di soppressione che regole di riepilogo. Quando l'integrazione viene configurata come connettore, le regole di soppressione e riepilogo vengono applicate prima dell'invio all'archivio registro eventi. Il controllo di soppressione e riepilogo va ad aggiungersi al controllo analogo eseguito nell'archivio registro eventi.

Ad esempio, è possibile applicare una regola di soppressione per far sì che gli eventi indesiderati di Windows non vengano inviati ad un agente WMI. Il traffico di rete verrà ridotto e questi eventi non raggiungeranno mai l'archivio registro eventi.

Importante: Creare ed utilizzare con attenzione le regole di soppressione, poiché impediscono la registrazione e la visualizzazione di alcuni eventi nativi. È consigliabile verificare le regole di soppressione in un ambiente di prova prima di distribuirle.

Per applicare le regole di soppressione e riepilogo

1. Aprire la procedura guidata di integrazione ed procedere al passaggio Regole di soppressione o Regole di riepilogo.
2. (Facoltativo) Per eseguire una ricerca delle regole disponibili, digitare il campo del modello di regole. Durante la digitazione, verranno visualizzate le regole corrispondenti ai criteri ricercati.
3. Selezionare le regole desiderate utilizzando il controllo pilota.
4. Fare clic sulla freccia appropriata per andare al passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Facendo clic su Salva e chiudi, nell'elenco della cartella utente verrà visualizzata la nuova integrazione; in caso contrario, verrà visualizzato il passaggio scelto dall'utente.

Ulteriori informazioni:

Attività relative alle regole per la soppressione e il riepilogo (a pagina 518)
Aggiunta di componenti dell'integrazione (a pagina 597)
Impostazione delle configurazioni predefinite (a pagina 599)
Impostazione delle configurazioni del registro file (a pagina 600)

Impostazione delle configurazioni predefinite

È possibile controllare le impostazioni di accesso ai dati dell'integrazione utilizzando le configurazioni predefinite. Ad esempio, è possibile impostare il controller di dominio cui connettersi per le comunicazioni WMI.

Questo passaggio non si applica alla creazione di un'integrazione syslog, dal momento che questo tipo di integrazione eredita i valori di configurazione dal listener syslog.

Per impostare le configurazioni predefinite

1. Aprire la procedura guidata di integrazione e proseguire fino al passaggio Configurazioni predefinite.
2. Completare i campi obbligatori.
3. (Facoltativo) Fare clic sul pulsante Nascondi accanto a qualsiasi configurazione predefinita per nascondere la configurazione durante la creazione di un connettore. Le configurazioni nascoste non sono visibili all'utente durante la creazione di un connettore basato su questa integrazione. Pertanto, è possibile impostare le configurazioni predefinite non modificabili quando si utilizza l'integrazione per distribuire un connettore.
4. Fare clic sulla freccia corretta per avanzare al passaggio della procedura guidata da completare in seguito, oppure fare clic su Salva e chiudi.

   Facendo clic su Salva e chiudi, nell'elenco della cartella utente verrà visualizzata la nuova integrazione; in caso contrario, verrà visualizzato il passaggio scelto dall'utente.

Ulteriori informazioni:

Aggiunta di componenti dell'integrazione (a pagina 597)

Impostazione delle configurazioni del registro file

È possibile controllare le impostazioni di accesso ai dati per l'integrazione tramite il sensore di registro file. È possibile utilizzare le impostazioni predefinite fornite da CA per la maggior parte degli intenti di raccolta eventi. È anche possibile alterare tali impostazioni per le integrazioni personalizzate.

Per impostare le configurazioni del registro file

1. Aprire la procedura guidata di integrazione, selezionare il tipo di sensore Registro file; quindi, procedere con il passaggio Configurazioni predefinite.
2. Impostare o modificare il tasso di ancoraggio per l'integrazione:

   UpdateAnchorRate

   Definisce la soglia, negli eventi, in cui si creerà un valore di ancoraggio. Se si interrompe l'elaborazione dell'evento, per iniziare nuovamente il calcolo, l'agente farà riferimento all'ultimo ancoraggio. Impostando un tasso di ancoraggio inferiore, si potrà ridurre l'eventualità della perdita di eventi, ma al prezzo di una riduzione delle prestazioni a causa della maggiore frequenza con cui si creerà il valore di ancoraggio. Impostando un alto tasso di ancoraggio, il carico di lavoro aumenterà poiché si rielaboreranno molti eventi nel caso in cui si interrompesse l'elaborazione.

   Impostazione predefinita: 4

   Leggi dall'inizio

   Controlla se, nel caso si interrompesse l'elaborazione dell'evento, l'agente dovrà iniziare la lettura del file dall'inizio. Se non si seleziona la casella di controllo, l'agente riprenderà la lettura degli eventi utilizzando il tasso di ancoraggio. Se si seleziona la casella di controllo, quando si distribuisce un connettore per la prima volta il sensore leggerà il file di registro dall'inizio. A seconda delle dimensioni del database e della velocità di generazione degli eventi, il sensore di registro di CA User Activity Reporting Module potrebbe impiegare del tempo per sincronizzarsi con gli eventi in tempo reale.

3. Impostare o modificare i seguenti valori di configurazione per l'origine evento specificata:

Directory di archiviazione file

Definisce il percorso in cui verrà salvato il file di registro dopo la rotazione. La directory di archiviazione ed il relativo nome possono essere uguali.

Flitro file

Definisce una stringa di testo utile per identificare il file di registro dell'origine evento. Il filtro file può utilizzare caratteri jolly. Ad esempio, per identificare un file di registro di nome messaggi.txt, è possibile inserire il filtro *messaggi** .

Tipo di rotazione file

Definisce l'integrazione in modo che essa corrisponda al tipo di rotazione file utilizzato dal prodotto da cui essa riceve gli eventi. Il tipo attuale di rotazione viene impostato da questo prodotto. Le seguenti impostazioni vengono supportate dalle integrazioni CA User Activity Reporting Module:

- NuovoFile : si utilizza quando l'obiettivo di integrazione viene ruotato da utility come rotazioneregistro.
- DimensioneFile: si utilizza quando l'obiettivo di integrazione si basa su una soglia di dimensione predefinita.
- DataFile: si utilizza quando l'obiettivo di integrazione si basa su un periodo di tempo predefinito. Di solito l'aggiornamento avviene a mezzanotte o dintorni.

Nome directory

Definisce il percorso per il file di registro dell'origine evento.

Delimitatore evento

Definisce l'espressione regolare che separa le singole voci di registro in un file di registro con più righe. Ogni volta che individua il delimitatore specificato, il sensore di registro avvia la lettura dei nuovi eventi. Questo consente a CA User Activity Reporting Module di ricevere più voci di eventi da un unico file di registro. Ad esempio, se ogni voce del file di registro contiene un indicatore di data e ora univoco, è possibile utilizzare l'espressione regolare come delimitatore per il formato di tale indicatore.

4. (Facoltativo) Per aggiungere ulteriori valori di origine evento, fare clic su Ripeti:

   Verrà visualizzato un gruppo aggiuntivo di campi dei valori di configurazione, utili per inserire i valori per la raccolta eventi da una diversa origine.

5. Fare clic sulla freccia appropriata per andare al passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, nell'elenco della cartella utente verrà visualizzata la nuova integrazione, oppure il passaggio scelto dall'utente.

Modalità di creazione di un listener syslog

È possibile utilizzare la procedura guidata listener per creare o modificare i listener syslog. Il listener controlla il modo in cui gli eventi syslog vengono instradati al server CA User Activity Reporting Module.

Nota: è possibile utilizzare il listener syslog di sottoscrizione (predefinito) per quasi tutti gli scopi. È possibile che alcuni utenti desiderino regolare la ricezione di syslog utilizzando listener personalizzati; per farlo, attenersi alle seguenti istruzioni.

Per utilizzare al meglio questa funzione avanzata è necessaria una conoscenza approfondita delle origini di eventi syslog nel proprio ambiente.

La creazione di un'integrazione include i passaggi seguenti:

1. Aprire la procedura guidata listener.
2. Aggiunta di componenti.
3. Selezione delle regole di soppressione.
4. Selezione delle regole di riepilogo.
5. Impostazione delle configurazioni predefinite.

Ulteriori informazioni:

Apertura della procedura guidata listener (a pagina 603)
Aggiunta di componenti listener (a pagina 604)
Impostazione delle configurazioni predefinite (a pagina 606)
Applicazione delle regole di soppressione e riepilogo (a pagina 605)
Aggiunta di un fuso orario syslog (a pagina 608)

Apertura della procedura guidata listener

Per creare un nuovo listener syslog o modificarne uno esistente, aprire la procedura guidata listener.

Per aprire la procedura guidata listener

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Raccolta registri.

   Viene visualizzato l'elenco della cartella Raccolta registri.

2. Fare clic sulla freccia accanto alla cartella Libreria di perfezionamento eventi per espanderla; quindi, selezionare la cartella Listener.

   I pulsanti di integrazione vengono visualizzati nel riquadro dei dettagli.

3. Fare clic su Nuovo listener:

   Viene visualizzata la procedura guidata listener.

   Mentre si utilizza la procedura guidata:

   - Fare clic su Salva per salvare il file senza chiudere la procedura;
   - Fare clic su Salva e chiudi per salvare il file e chiudere la procedura;
   - Fare clic su Ripristina per ripristinare la visualizzazione della procedura alle ultime impostazioni salvate.

Aggiunta di componenti listener

Per creare un listener syslog, impostare le informazioni come ad esempio la guida alla configurazione e il nome.

Per aggiungere componenti listener

1. Aprire la procedura guidata listener.
2. Immettere un nome per il nuovo listener.
3. (Facoltativo) Selezionare il componente seguente dall'elenco a discesa:

   Assistente di configurazione

   Indica il file binario dell'assistente utilizzato dall'integrazione per connettersi all'archivio di registro selezionato. Molte integrazioni non richiedono un assistente di configurazione.

   Nota: il tipo di sensore di un listener è sempre syslog.
4. (Facoltativo) Digitare una descrizione del listener.
5. Fare clic sulla freccia appropriata per andare al passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Facendo clic su Salva e chiudi, nell'elenco della cartella utente verrà visualizzata la nuova integrazione; in caso contrario, verrà visualizzato il passaggio scelto dall'utente.

Applicazione delle regole di soppressione e riepilogo

È possibile applicare le regole di soppressione e riepilogo a un listener syslog per semplificare il perfezionamento degli eventi. Quando si utilizza il listener con un connettore, gli eventi in entrata vengono verificati secondo le regole di soppressione e riepilogo prima di essere inviati a CA User Activity Reporting Module.

Ad esempio, se si desidera creare un listener che riceve solamente gli eventi di CA Access Control, è possibile applicare la regola per l'accesso riuscito ai file CA Access Control. In questo modo, si evita un'elaborazione eccessiva, poiché solo le regole necessarie vengono utilizzate per verificare gli eventi in arrivo.

Importante: Creare e utilizzare le regole di soppressione con cautela perché impediscono la registrazione e la visualizzazione completa di determinati eventi nativi. È consigliabile verificare le regole di soppressione in un ambiente di prova prima di distribuirle.

Applicazione di una regola di soppressione o riepilogo

1. Aprire la procedura guidata di listener e procedere con il passaggio Regole di soppressione o con il passaggio Regole di riepilogo.
2. (Facoltativo) Digitare nel campo del modello delle regole per ricercare le regole disponibili. Mentre si digita vengono visualizzare le regole che corrispondono a quanto immesso.
3. Selezionare le regole desiderate utilizzando il controllo pilota.
4. Fare clic sulla freccia appropriata per andare al passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Facendo clic su Salva e chiudi, nell'elenco della cartella utente verrà visualizzato il nuovo listener; in caso contrario, verrà visualizzato il passaggio scelto dall'utente.

Impostazione delle configurazioni predefinite

È possibile controllare le impostazioni di accesso ai dati del listener syslog utilizzando le configurazioni predefinite. Ad esempio, è possibile impostare gli host attendibili o le porte di comunicazione predefinite.

Per impostare le configurazioni predefinite

1. Aprire la procedura guidata listener e proseguire fino al passaggio Configurazioni predefinite.
2. Modificare o aggiungere i valori desiderati, includendo:

   Ordinamento evento

   Assicura che gli eventi vengano inviati all'archivio di registro eventi nello stesso ordine in cui vengono ricevuti. Se questa opzione è disabilitata, l'ordine può cambiare se alcuni eventi vengono analizzati e inviati più rapidamente di altri. L'abilitazione di Ordinamento evento può influenzare le prestazioni, poiché rallenta l'elaborazione e l'invio degli eventi.

   Conteggio dei thread per coda

   Definisce il numero di thread di elaborazione per ogni protocollo. L'utilizzo di molti thread di elaborazione rende più veloce l'elaborazione stessa se l'ordinamento eventi è disabilitato. Se invece l'ordinamento eventi è abilitato, il numero di thread non inciderà in alcun modo. L'utilizzo di molti thread può incidere sulle prestazioni.

   Dimensioni coda

   Imposta le dimensioni della coda in base al numero di eventi per le informazioni sugli eventi in arrivo. La coda viene utilizzata per l'elaborazione e l'invio di eventi. Se il buffer si riempie non sarà possibile ricevere ulteriori eventi, finché gli eventi elaborati non lasceranno spazio.

Porte

Imposta le porte utilizzate dal listener per ricevere gli eventi tramite UDP o TCP. Se vengono specificate più porte, il servizio prova a collegarsi a ognuna a turno. Le porte syslog predefinite sono già impostate. Se gli eventi syslog sono stati indirizzati ad altre porte, occorre impostare di conseguenza le porte di ricezione CA User Activity Reporting Module.

Importante: Se l'agente è in esecuzione su un sistema UNIX come utente non root, modificare le porte del listener syslog immettendo numeri di porta superiori a 1024. In questo caso, la porta UDP 514, predefinita, non è aperta e non viene raccolto alcun evento syslog.

Host attendibile

Indica gli indirizzi IP attendibili per IPv4 o IPv6. Vengono accettate solo le comunicazioni provenienti da un host attendibile. Se non si specificano host attendibili, verranno accettati eventi da tutte le origini evento syslog disponibili. È necessario immettere l'indirizzo IP esatto registrato nel campo event_source_address per gli host attendibili. Non sono ammessi caratteri jolly o indirizzi di sottorete.

Fusi orari

Consente di aggiungere fusi orari per i computer dell'origine eventi syslog. In genere, syslog non registra l'ora. Identificare i sistemi di origine per indirizzo IP completo e fuso orario per ricevere e regolare gli eventi provenienti da origini syslog che si trovano in un fuso orario diverso rispetto al server CA User Activity Reporting Module. Non elencare origini syslog nello stesso fuso orario del server.

3. Fare clic sulla freccia appropriata per andare al passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Facendo clic su Salva e chiudi, nell'elenco della cartella utente verrà visualizzato il nuovo listener; in caso contrario, verrà visualizzato il passaggio scelto dall'utente.

Aggiunta di un fuso orario syslog

Aggiungere un fuso orario per consentire a uno o più computer di origine evento syslog di ricevere e regolare correttamente gli eventi dalle origini syslog situate in un fuso orario diverso rispetto al server CA User Activity Reporting Module.

È possibile aggiungere un fuso orario syslog durante la creazione di un'integrazione, la configurazione di un connettore o la creazione di una configurazione salvata.

Nota: se si aggiunge un fuso orario ad un ambiente che applica l'ora legale, verificare l'esistenza di una voce di fuso orario corrispondente sul sistema host dell'agente. In assenza di tale voce, il fuso orario di syslog non sarà in grado di elaborare il passaggio all'ora legale e gli eventi presenteranno un indicatore di orario non corretto durante il periodo dell'ora legale.

Per aggiungere un fuso orario syslog

1. Accedere all'interfaccia del fuso orario syslog in uno dei seguenti modi:
   - Aprire l'integrazione di syslog a cui aggiungere i fusi orari e procedere al passaggio Configurazione predefinita.
   - Aprire il connettore di syslog a cui aggiungere i fusi orari e procedere al passaggio Configurazione connettore.
   - Aprire la configurazione salvata a cui aggiungere i fusi orari.

   Viene visualizzata l'interfaccia del fuso orario syslog.
2. Fare clic su Crea cartella nell'area Fusi orari

   Nell'area dell'elenco viene visualizzato un nuovo fuso orario e un elenco a discesa dei fusi compare nel riquadro di destra.
3. Scegliere un fuso orario dall'elenco a discesa.

   Il fuso orario selezionato verrà visualizzato accanto alla cartella.
4. Fare clic sulla freccia accanto alla cartella.

   La cartella si espande e mostra per quel fuso orario un singolo computer origine evento senza titolo.
5. Selezionare l'icona del computer.

   Viene visualizzato il campo di immissione Indirizzo IP.
6. Immettere un indirizzo IP.

   L'indirizzo verrà visualizzato accanto all'icona del computer durante la digitazione.

7. (Facoltativo) Per aggiungere altri computer di origine evento, selezionare un'origine evento esistente e fare clic su Aggiungi elemento.

   La cartella si chiude. Aprirla per visualizzare un nuovo computer origine evento senza titolo. Andare al passaggio 6.

8. (Facoltativo) Per aggiungere altri fusi orari, fare clic su Crea cartella.

   Viene visualizzata una nuova cartella senza titolo per il fuso orario. Andare al passaggio 3.

9. Una volta create tutte le cartelle del fuso orario e gli elementi di indirizzo dell'origine eventi desiderati, fare clic su Salva.

Ulteriori informazioni:

Impostazione della configurazione di un connettore (a pagina 615)
Creazione di una configurazione salvata (a pagina 620)

Creazione di una nuova versione di integrazione

È possibile creare una nuova versione di un'integrazione esistente creata dagli utenti (personalizzata).

Per creare una nuova versione di integrazione

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria.
2. Espandere le cartelle Integrazione Log e Integrazioni e passare alla cartella utente che contiene l'integrazione desiderata.
3. Selezionare l'integrazione utente e fare clic su Crea nuova versione.
4. Viene visualizzata la procedura guidata di nuova integrazione, che mostra i dettagli dell'integrazione selezionata.
5. Apportare le modifiche desiderate e fare clic su Salva e chiudi.

   La nuova versione dell'integrazione viene visualizzata nell'elenco.

Eliminazione di un'integrazione

È possibile eliminare un'integrazione personalizzata. Non è possibile eliminare un'integrazione di sottoscrizione.

Per eliminare un'integrazione personalizzata

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria.
2. Espandere le cartelle Integrazione Log e Integrazioni e passare alla cartella utente che contiene l'integrazione da eliminare.
3. Fare clic sull'integrazione che si desidera eliminare dall'elenco.
4. Fare clic su Elimina nella parte superiore dell'elenco.

   Viene visualizzata una finestra di conferma.
5. Fare clic su Sì.

   L'integrazione viene rimossa dall'elenco.

Esportazione e importazione delle definizioni delle integrazioni

È possibile esportare e importare i dettagli delle integrazioni per utilizzarli in altri server di gestione. In questo modo, è possibile trasferire correttamente integrazioni personalizzate in altri ambienti CA User Activity Reporting Module, oppure da un ambiente di prova a uno attivo.

Ulteriori informazioni

Importazione delle definizioni delle integrazioni (a pagina 611)
Esportazione delle definizioni delle integrazioni (a pagina 611)

Importazione delle definizioni delle integrazioni

È possibile importare i file XML con le definizioni delle integrazioni da utilizzare nel server di gestione locale.

Per importare i dettagli delle integrazioni

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Raccolta registri.

   Viene visualizzata la struttura della cartella Raccolta registri.

2. Espandere la cartella Integrazioni e andare alla sottocartella in cui si vuole importare un'integrazione.

3. Fare clic su Importa integrazione.

   Viene visualizzata la finestra di dialogo Importa file.

4. Immettere o individuare la posizione in cui importare il file, quindi fare clic su OK.

   I file delle query vengono importati nella cartella corrente, quindi viene visualizzata una finestra di dialogo di conferma.

5. Fare clic su OK.

Esportazione delle definizioni delle integrazioni

È possibile esportare i dettagli delle integrazioni per utilizzarle in altri server di gestione. Il file di esportazione viene salvato in formato XML.

Per esportare i dettagli delle integrazioni

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Raccolta registri.

   Viene visualizzata la struttura della cartella Raccolta registri.

2. Espandere la cartella Integrazioni e andare alla sottocartella contenente l'integrazione da esportare.

3. Fare clic su Esporta integrazioni.

Viene visualizzata un finestra di download.

4. Immettere o selezionare la posizione in cui salvare i file di esportazione XML, quindi fare clic su Salva.

   I file delle query vengono salvati nella posizione selezionata, quindi viene visualizzata una finestra di conferma.

5. Fare clic su OK.

Modalità di creazione di un connettore

È possibile creare un connettore per la raccolta di eventi da un determinato sistema operativo o dispositivo nel proprio ambiente. Si usa un'integrazione o un listener come modello per la creazione di un connettore utilizzando la nuova procedura guidata del connettore. Ogni nuovo connettore viene applicato a un agente del proprio ambiente.

È possibile creare connettori di diversi tipi, tra cui integrazioni WMI e ODBC, che raccolgono attivamente eventi del tipo specificato. È anche possibile creare connettori syslog che ricevano passivamente gli eventi. I connettori syslog possono ricevere eventi da più origini, a differenza degli altri tipi. Perciò il processo di creazione di un connettore syslog è leggermente diverso.

Il processo di creazione di un connettore comprende i passaggi riportati di seguito:

1. Apertura della creazione guidata del connettore.
2. Aggiunta di dettagli sul connettore, come la selezione del listener per i connettori syslog.
3. Applicazione delle regole di soppressione.
4. Applicazione delle regole di riepilogo.
5. Impostazione delle configurazioni del connettore.

Ulteriori informazioni:

Apertura della creazione guidata del connettore (a pagina 613)
Aggiunta di dettagli al connettore (a pagina 613)
Applicazione delle regole di soppressione e riepilogo (a pagina 614)
Impostazione della configurazione di un connettore (a pagina 615)

Apertura della creazione guidata del connettore

Per creare un nuovo connettore o modificarne uno esistente, è necessario aprire la creazione guidata del connettore.

Per aprire la creazione guidata del connettore

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Raccolta registri.

   Viene visualizzato l'elenco della cartella Raccolta registri.

2. Espandere la cartella Explorer agente e selezionare il gruppo di agenti in cui si vuole aggiungere o modificare un connettore.

   Vengono visualizzati gli agenti che appartengono al gruppo selezionato.

3. Selezionare l'agente in cui si desidera aggiungere o modificare un connettore.

   I pulsanti per la gestione dell'agente vengono visualizzati nel riquadro dei dettagli.

4. Fare clic su Nuovo connettore:

   Viene visualizzata la creazione guidata del connettore.

   Mentre si utilizza la procedura guidata:

   - Fare clic su Salva per salvare il file senza chiudere la procedura.
   - Fare clic su Salva e chiudi per salvare il file e chiudere la procedura.
   - Fare clic su Ripristina per ripristinare la visualizzazione della procedura alle ultime impostazioni salvate.

Aggiunta di dettagli al connettore

È possibile aggiungere un nome e una descrizione per identificare meglio il connettore. Occorre anche scegliere l'integrazione da usare come modello per il connettore.

Per aggiungere dettagli al connettore

1. Aprire la procedura guidata di progettazione del connettore.

   Una volta visualizzata, la procedura mostra nella parte superiore dello schermo la piattaforma e la versione piattaforma dell'agente corrente.

2. Specificare un nome per il connettore.
3. Selezionare il pulsante di opzione Listener se si vuole creare un connettore syslog, oppure Integrazione per tutti gli altri tipi di connettore.
4. Selezionare l'integrazione da utilizzare come modello. L'elenco a discesa Integrazione mostra tutte le integrazioni disponibili per la versione corrente della piattaforma e il tipo di origine evento.
5. (Facoltativo) Selezionare Controllo di versione piattaforma bypass per creare integrazioni per *tutte* le versioni della piattaforma agente disponibili nell'elenco a discesa Integrazione.
6. Inserire una descrizione per il connettore.
7. Procedere con il passaggio che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, il connettore viene visualizzato nell'elenco dei connettori.

Applicazione delle regole di soppressione e riepilogo

Quando si crea o modifica un connettore, è possibile selezionare le regole di soppressione e riepilogo da applicare agli eventi gestiti dal connettore. Le regole di soppressione o riepilogo aggiunte vengono applicate prima che gli eventi vengano trasmessi al server CA User Activity Reporting Module.

Applicazione delle regole di soppressione o riepilogo

1. Aprire la procedura guidata di progettazione dei connettori e procedere con il passaggio Applica regole di soppressione o con il passaggio Regole di riepilogo.

   Viene visualizzato un elenco delle regole di soppressione disponibili.
2. (Facoltativo) Digitare nel campo del modello delle regole per ricercare le regole disponibili. Mentre si digita vengono visualizzare le regole che corrispondono a quanto immesso.
3. Selezionare la regola o le regole che si desidera applicare utilizzando il controllo pilota.
4. Procedere con il passaggio che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, il connettore viene visualizzato nell'elenco dei connettori.

Impostazione della configurazione di un connettore

Al momento di creare o modificare un connettore, è possibile impostare configurazioni individuali che determinino in che modo il connettore riceve e trasmette gli eventi. È possibile impostare configurazioni per ogni connettore oppure utilizzare configurazioni salvate.

Le configurazioni salvate sono raccolte di impostazioni di accesso dati che è possibile riutilizzare. È possibile applicare le configurazioni salvate a più connettori.

Per impostare le configurazioni dei connettori

1. Aprire la procedura guidata di progettazione del connettore e proseguire fino al passaggio Configurazione connettore.
2. Se è stato selezionato il sensore di registro/listener syslog, scegliere l'integrazione o le integrazioni che il connettore dovrà utilizzare.
3. Selezionare le configurazioni salvate desiderate dall'elenco a discesa, oppure modificare i valori di configurazione visualizzati. I connettori ereditano le loro impostazioni di configurazione dall'integrazione o, nel caso dei connettori syslog, dal listener.
4. (Facoltativo) Fare clic sul collegamento ? per visualizzare la guida del connettore per l'integrazione selezionata. La guida visualizzata fornisce informazioni aggiuntive.
5. Fare clic su Salva e chiudi.

   Il connettore viene visualizzato nell'elenco dei connettori.

Impostazione della CPU del connettore

Durante il processo di creazione o modifica di un connettore è possibile limitare l'utilizzo della CPU del connettore. La ricezione degli eventi da parte del sensore log CA User Activity Reporting Module viene attivata in base all'utilizzo di CPU allocato.

Importante: si sconsiglia di impostare una percentuale di utilizzo della CPU superiore all'80%, in quanto valori elevati potrebbero compromettere le prestazioni di CA User Activity Reporting Module.

Procedere come descritto di seguito:

1. Aprire la progettazione guidata del connettore e proseguire fino al passaggio Impostazioni del connettore CPU.
2. Selezionare Abilita rallentamento CPU.
3. Immettere la percentuale di CPU che potrà essere utilizzata dal connettore nel campo Percentuale per CPU.

   Nota: per impostazione predefinita, CA User Activity Reporting Module mostra il numero di CPU configurate durante l'installazione.
4. Fare clic su Salva e chiudi.

   Il connettore viene visualizzato nell'elenco dei connettori.

   Nota: CA User Activity Reporting Module richiede un tempo minimo di cinque minuti per applicare le modifiche apportate all'utilizzo della CPU.

Visualizzazione di un connettore

È possibile aprire l'elenco dei connettori per ogni agente per visualizzare e modificare i connettori a esso associati.

Per visualizzare un connettore

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Raccolta registri.

   Viene visualizzato l'elenco della cartella Raccolta registri.

2. Espandere Explorer agente e le cartelle dei gruppi di agenti per visualizzare i singoli elementi.

3. Selezionare l'agente su cui è presente il connettore da visualizzare.

4. Fare clic su Visualizza connettori:

   Viene visualizzato l'elenco Connettori agente, che mostra i connettori distribuiti sull'agente selezionato.

Visualizzazione di una guida per il connettore

È possibile visualizzare una guida contenente informazioni per l'installazione e configurazione per ogni tipo di connettore CA User Activity Reporting Module. La guida contiene istruzioni su come configurare il prodotto target e il connettore stesso in modo da ricevere eventi.

Contiene inoltre informazioni di riferimento quali i nomi dei log del connettore e i tipi di eventi che il connettore trasmette a CA User Activity Reporting Module.

Per visualizzare una guida per il connettore

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria.

2. Espandere le cartelle Libreria di trattamento eventi, Integrazioni e Sottoscrizione per rivelare le singole integrazioni.

3. Selezionare l'integrazione che si desidera usare per creare un connettore.

   I dettagli dell'integrazione vengono visualizzati nel riquadro di destra.

4. Fare clic sul collegamento ? azzurro sopra a Nome integrazione.

   La guida per il connettore per quell'integrazione appare in una nuova finestra del browser.

Modifica di un connettore

È possibile modificare un connettore esistente. La modifica di un connettore crea una nuova versione.

Per modificare un connettore

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Raccolta registri.

   Viene visualizzato l'elenco della cartella Raccolta registri.

2. Espandere Explorer agente e le cartelle dei gruppi di agenti per visualizzare i singoli elementi.

3. Selezionare l'agente su cui è presente il connettore da visualizzare.

4. Fare clic su Visualizza connettori:

   Viene visualizzato l'elenco Connettori agente, che mostra i connettori presente sull'agente selezionato.

5. Fare clic su Modifica accanto al connettore da modificare.

   Viene avviata la creazione guidata del connettore, che mostra il connettore selezionato.

6. Eseguire le modifiche desiderate e fare clic su Salva e chiudi.

   Il connettore modificato viene visualizzato nell'elenco.

Informazioni sulle configurazioni salvate

Una configurazione salvata è una raccolta riutilizzabile di impostazioni che consente a un connettore di raccogliere eventi da un dispositivo o da un'origine di registro. È possibile utilizzare le configurazioni salvate per consentire un livello di personalizzazione che non richieda la creazione di un'integrazione completamente nuova.

Le configurazioni si differenziano in base al tipo di integrazione. Ad esempio, è possibile salvare gli host attendibili per un connettore syslog, o le informazioni di contatto di un server WMI per un connettore WMI.

Le configurazioni salvate consentono di memorizzare queste informazioni raggruppate e di applicarle a più connettori. Dato che ogni configurazione salvata è associata a un'integrazione specifica, è possibile utilizzarla soltanto sui connettori che usano tale integrazione.

Ulteriori informazioni

Creazione di una configurazione salvata (a pagina 620)
Attività relative a integrazioni e connettori (a pagina 593)

Creazione di una configurazione salvata

È possibile creare una configurazione salvata associandola a un'integrazione specifica.

Per creare una configurazione salvata

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Raccolta registri.

   Viene visualizzato l'elenco della cartella Raccolta registri.

2. Aprire la cartella Libreria di perfezionamento eventi e andare all'integrazione in cui si desidera creare una configurazione salvata.

   I dettagli dell'integrazione vengono visualizzati nel riquadro dei dettagli.

3. Fare clic su Configurazioni salvate:

   Viene visualizzato l'elenco Configurazioni salvate.

4. Fare clic su Nuovo.

   Viene visualizzata la finestra di dialogo Configurazione salvata, che mostra i valori di configurazione predefiniti per l'integrazione selezionata.

5. Inserire i valori di configurazione desiderati e fare clic su Salva e chiudi.

   Verrà visualizzato un messaggio di conferma.

6. Fare clic su OK.

   La configurazione salvata viene visualizzata nell'elenco.

Come configurare i connettori in blocco

È possibile configurare le origini di raccolta evento creando più connettori in blocco. È possibile creare più connettori contemporaneamente utilizzando le stesse integrazioni e distribuendole a diversi agenti del proprio ambiente.

Il processo di configurazione comprende la selezione delle origini evento, l'applicazione delle regole di soppressione e riepilogo e l'impostazione delle configurazioni di connettore. Per poter sfruttare questa funzionalità, creare un elenco di informazioni di identificazione, ad esempio nomi di host ed indirizzi IP delle origini evento da configurare. L'elenco deve essere in formato valori separati da virgola (.csv).

Il processo di configurazione delle origini di raccolta tramite la procedura guidata di distribuzione dei connettori in blocco è composto dai seguenti passaggi:

1. Aprire la procedura guidata di distribuzione dei connettori in blocco
2. Selezionare le informazioni di origine
3. Applicare le regole di soppressione
4. Applicare le regole di riepilogo
5. Configurare le impostazioni del connettore
6. Selezionare le origini di mapping e gli agenti

Ulteriori informazioni:

Aprire la procedura guidata Configura origini di raccolta. (a pagina 622)
Selezionare Dettagli origine (a pagina 623)
Applicazione delle regole di soppressione (a pagina 624)
Applicazione di regole di riepilogo (a pagina 624)
Configurazione connettore (a pagina 625)
Selezionare gli agenti e mappare le origini (a pagina 626)

Aprire la procedura guidata Configura origini di raccolta.

Per creare connettori sugli agenti, utilizzare la procedura guidata distribuzione connettori in blocco.

Per aprire la procedura guidata distribuzione connettori in blocco

1. Fare clic sulla scheda Amministrazione, e quindi sulla sottoscheda Raccolta registri.

   Verrà visualizzato l'elenco cartella di Raccolta registri.

2. Fare clic sulla cartella Explorer agente, quindi su Configura origini di raccolta:

   Verrà visualizzata la procedura guidata Configura origini di raccolta:

   Quando si utilizza la procedura guidata:

   - Fare clic su Salva per applicare gli aggiornamenti senza chiudere la procedura guidata. Viene visualizzato un messaggio di conferma.
   - Fare clic su Salva e chiudi per applicare gli aggiornamenti e chiudere la procedura guidata. Non verrà visualizzato alcun messaggio di conferma.

Selezionare Dettagli origine

Selezionare i dettagli origine e identificare l'integrazione da connettere alle origini eventi. Per completare il passaggio, è necessario disporre di un elenco dei necessari dettagli origine evento in un file .csv.

Nota: il file .csv contiene le informazioni necessarie per la creazione dei connettori. Ogni colonna nel file .csv identifica un campo per la configurazione di un connettore e contiene i valori di quel campo. Ad esempio, potrebbe esistere una colonna Indirizzo IP con elencati gli indirizzi IP degli host dai quali si desidera ricevere eventi.

La sezione Come creare un'integrazione (a pagina 595) contiene campi di configurazione specifici per tipo di sensore di registro.

Per selezionare dettagli origine

1. Aprire la procedura guidata distribuzione connettori in blocco.
2. Dall'elenco a discesa Integrazione, selezionare l'integrazione utilizzata dalle origini.
3. Dall'elenco a discesa Versione, selezionare la versione corretta dell'integrazione.
4. Individuare il percorso in cui è stato salvato il file di origine di raccolta da utilizzare. L'origine di raccolta deve essere un file .csv.

   Nell'area Contenuti file di origine, verranno visualizzate per la verifica le prime 100 righe del file di origine di raccolta selezionato. La prima riga è impostata come riga di intestazione della colonna e rimane tale anche se si regola la dimensione campione al passaggio 5.
5. Utilizzare gli elenchi a discesa Dalla riga e Alla riga per ridurre la parte del file di origine di raccolta da utilizzare.

   Nell'area Contenuti file di origine, verrà visualizzata a scopo di verifica la parte selezionata del file di origine di raccolta. Le intestazioni delle colonne non verranno influenzate se si modifica il valore Dalla riga con un valore maggiore di 1.
6. Proseguire con il passaggio successivo.

Ulteriori informazioni:

Modalità di creazione di un'integrazione (a pagina 595)

Applicazione delle regole di soppressione

È possibile selezionare le regole di soppressione da applicare alle modifiche di configurazione in blocco.

Per applicare le regole di soppressione

1. Aprire la procedura guidata distribuzione connettori in blocco e accedere al passaggio Applica regole di soppressione.
2. Selezionare le regole da applicare tra quelle disponibili, utilizzando il controllo pilota.

   Nota: è possibile cercare le regole di soppressione tramite il campo Modello regole di soppressione.
3. Proseguire con il passaggio successivo.

Applicazione di regole di riepilogo

È possibile selezionare le regole di riepilogo da applicare alle modifiche di configurazione in blocco.

Per applicare le regole di riepilogo

1. Aprire la procedura guidata distribuzione connettori in blocco e accedere al passaggio Applica regole di riepilogo.
2. Selezionare le regole da applicare tra quelle disponibili, utilizzando il controllo pilota.

   Nota: è possibile ricercare le regole di riepilogo tramite il campo Modello regole di riepilogo.
3. Proseguire con il passaggio successivo.

Configurazione connettore

È possibile impostare le configurazioni del connettore per la creazione della connessione in blocco. Ciascun connettore creato condivide le configurazioni impostate in questo passaggio, utilizzando le origini raccolte dal file .csv al Passaggio 1 oppure le Configurazioni salvate.

Per impostare le configurazioni dei connettori

1. Aprire la procedura guidata distribuzione connettori in blocco e accedere al passaggio Configurazione connettore.

   La pagina visualizzerà i Campi di origine impostati al passaggio 1. Ciascuna colonna di intestazione del file di origine verrà visualizzata come campo di origine. Inoltre, nell'area Configurazione sensore della pagina saranno visualizzate le configurazioni del sensore predefinite per l'integrazione selezionata.

2. Impostare la configurazione connettore in uno dei seguenti modi:

   - Selezionare una Configurazione salvata dal relativo elenco a discesa.
   - Nell'area Configurazione sensore, impostare singole configurazioni trascinando le voci del campo di origine nei campi di configurazione desiderati. Impostare manualmente tutti i campi necessari per i quali non sono presenti valori campo di origine.

     Ad esempio, l'elenco di origine contiene una colonna Nome utente. Se esiste un nome utente per il tipo di sensore che si sta configurando, trascinare la colonna nel campo Configurazione sensore nome utente.

3. (Facoltativo) Fare clic su Ripeti per aggiungere ulteriori campi Configurazione sensore secondo necessità.

4. Proseguire con il passaggio successivo.

Selezionare gli agenti e mappare le origini

È possibile selezionare gli agenti nei quali si desidera creare i connettori configurati. Mappare le origini evento selezionate al passaggio 1 per gli agenti cui è diretta la distribuzione dei connettori.

Selezionare gli agenti e mappare le origini

1. Aprire la procedura guidata distribuzione connettori in blocco e procedere al passaggio Selezionare agenti e mappare le origini.

   Verrà visualizzato un elenco di origini basato sulle origini caricate al Passaggio 1. Ogni origine è numerata per riga, quindi Origine 1 rappresenta la prima riga specificata nell'elenco.

2. Ricercare gli agenti di destinazione per Gruppo agenti, Piattaforma o Nome agente.

3. Trascinare una o più origini desiderate nella cartella di ciascun agente di destinazione e fare clic per salvare il mapping del connettore.

4. Fare clic su Salva oppure su Salva e chiudi.

   I connettori basati sulle origini selezionate dall'utente sono configurati sugli agenti selezionati.

Aggiornamento delle configurazioni di più connettori

È possibile aggiornare più connettori che utilizzano lo stesso sensore di log per modificare una o più configurazioni predefinite. Ad esempio, si potrebbe cambiare il tipo di rotazione del file di log su più connettori utilizzando il sensore del file di log.

Per aggiornare le configurazioni di più connettori

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria.
2. Espandere le cartelle Integrazione Log, Integrazioni e Sottoscrizione.
3. Selezionare un'integrazione che utilizza il sensore log del tipo al quale si desidera applicare le modifiche alla configurazione.
4. Fare clic su Applica aggiornamento batch ai connettori:

   Appare la procedura guidata aggiornamento connettori, che visualizza la pagina Seleziona connettori.
5. Selezionare i connettori ai quali applicare gli aggiornamenti e passare alla pagina Configurazioni predefinite.
6. Immettere il valore desiderato in ogni campo da aggiornare e selezionare la casella di controllo corrispondente.
7. Fare clic su Esegui.

   Viene visualizzato un messaggio di conferma.

Capitolo 17: Correlazione eventi e Gestione incidenti

Questa sezione contiene i seguenti argomenti:

Attività delle regole di correlazione (a pagina 631)
Attività di gestione incidenti (a pagina 645)
Visualizzazione di dettagli su un incidente (a pagina 646)

Capitolo 18: Attività delle regole di correlazione

Le regole di correlazione possono segnalare modelli di eventi, consentendo di identificare attività sospette o condizioni pericolose nel proprio ambiente. Ogni volta che gli eventi corrispondono ai criteri di una regola di correlazione, CA User Activity Reporting Module crea un incidente.

Se si dispone del ruolo di amministratore, è possibile eseguire le seguenti attività relative alle regole di correlazione:

- Creare, modificare o eliminare una regola di correlazione
- Creare un gruppo di regole di correlazione
- Importare o esportare una regola di correlazione.
- Applicare regole di correlazione e associare destinazioni di notifica nel proprio ambiente.

Questa sezione contiene i seguenti argomenti:

Informazioni sulle regole di correlazione (a pagina 632)
Utilizzo di regole di correlazione predefinite (a pagina 633)
Utilizzo degli elenchi con chiave con le regole di correlazione (a pagina 637)
Esempio: creazione di un file CSV per il test (a pagina 638)
Informazioni sulle notifiche di incidente (a pagina 638)
Come progettare e applicare le notifiche di incidente (a pagina 640)

Informazioni sulle regole di correlazione

È possibile applicare le regole di correlazione predefinite, utilizzare la procedura guidata per creare regole di correlazione personalizzate per il proprio ambiente oppure modificare le regole esistenti. Le regole di correlazione consentono di identificare gruppi di eventi che potrebbero indicare attacchi o altri rischi per la sicurezza. Per creare o modificare le regole di correlazione è necessario disporre del ruolo di Amministratore.

Quando si crea una regola di correlazione, è necessario selezionare quale dei tre tipi di regola si desidera creare. Il modello della regola controlla l'evento o gli eventi che vengono considerati un incidente. Sono disponibili i modelli indicati di seguito:

- Filtro semplice: consente di ricercare un singolo evento o stato. Questo modello crea un incidente da un singolo evento.
- Modello Conteggio: consente di ricercare un insieme di eventi identici. È possibile controllare il numero di eventi dello stesso tipo ricercati dalla regola. Ogni volta che la regola rileva il numero di eventi impostato, viene generato un incidente.
- Modello Transizione di stato: consente di ricercare una serie di eventi correlati. Quando si verifica un evento o uno stato specifico, seguito da uno o più eventi o stati, la regola crea un incidente. È possibile definire gli stati ricercati dalla regola e impostare il numero di stati.

Nota: la correlazione effettiva richiede la visualizzazione completa degli eventi in entrata. Per questa ragione si sconsiglia di applicare le regole di soppressione e aggregazione a livello agente. Gli eventi soppressi o aggregati a livello dell'agente non vengono inclusi nella correlazione e nella creazione incidente.

La correlazione eventi può determinare un elevato traffico di rete, si consiglia pertanto di assegnare un server di correlazione dedicato. Per ulteriori informazioni sui ruoli del server, consultare la *Guida all'implementazione di CA User Activity Reporting Module*.

In caso di un numero elevato di messaggi incidente da elaborare, il servizio di correlazione può mantenere in attesa fino a un massimo di 10.000 messaggi. Una volta raggiunto questo limite, i messaggi in eccesso vengono eliminati. In tal caso, CA User Activity Reporting Module genera eventi con monitoraggio automatico.

Ulteriori informazioni:

Informazioni sulle notifiche di incidente (a pagina 638)

Utilizzo di regole di correlazione predefinite

CA User Activity Reporting Module fornisce un ampio numero di regole di correlazione predefinite da utilizzare nel proprio ambiente, organizzate per tipo o per requisiti normativi. Ad esempio, nella cartella Regole di correlazione dell'interfaccia Libreria è presente una cartella denominata PCI, contenente le regole per vari requisiti PCI. È inoltre presente una cartella denominata Identità, che contiene le regole generiche per l'autenticazione e l'autorizzazione.

Esistono tre tipi principali di regole, che è possibile includere tutte o singolarmente in ciascuna categoria. Questo argomento fornisce un esempio di scelta e applicazione di una regola di ogni tipo.

Esempio: selezione e applicazione di una regola semplice

Le regole di correlazione semplici consentono di rilevare la presenza di uno stato o un'occorrenza. Ad esempio, è possibile applicare una regola che avvisi per le eventuali attività di creazione account al di fuori del normale orario di ufficio. Prima di applicare una regola, è necessario verificare di aver creato le destinazioni di notifica desiderate per il proprio ambiente.

Per selezionare e applicare la regola Creazione account al di fuori delle ore lavorative

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria ed espandere la cartella Regole di correlazione.
2. Espandere la cartella PCI, quindi la cartella Requisito 8 e selezionare la regola Creazione account al di fuori delle ore lavorative.

   I dettagli della regola verranno visualizzati nel riquadro a destra.
3. Rivedere i dettagli della regola per verificare che sia appropriata per il proprio ambiente. In questo caso, i filtri consentono di definire l'azione di creazione account e impostare l'orario lavorativo normale per ora e giorno della settimana.
4. (Facoltativo) Fare clic su Modifica nella parte superiore del riquadro per modificare le impostazioni del filtro, se necessario. Ad esempio, è possibile modificare l'orario lavorativo normale in base alle specifiche del proprio ambiente.

   Viene visualizzata la procedura guidata di gestione delle regole, popolata con i dettagli della regola.
5. Aggiungere i dettagli di notifica desiderati nella procedura guidata. I dettagli di notifica forniscono il contenuto del messaggio che verrà inviato come specificato in Destinazioni di notifica.

6. Dopo aver terminato la preparazione della regola, fare clic su Salva e chiudi. Quando si modifica e si salva una regola di correlazione predefinita, CA User Activity Reporting Module crea automaticamente una nuova versione, preservando la versione originale.
7. Fare clic sulla sottoscheda Servizi e quindi espandere il nodo Servizio di correlazione.
8. Selezionare il server a cui si desidera applicare la regola. Se si dispone di un server identificato come server di correlazione, selezionare tale server.
9. Fare clic su Applica nell'area Configurazione regola, quindi selezionare la nuova versione della regola Creazione account al di fuori delle ore lavorative, con la destinazione di notifica desiderata associata alla regola.
10. Fare clic su OK per chiudere la finestra di dialogo e attivare la regola.

Esempio: selezione e applicazione di una regola di conteggio

Le regole di correlazione di conteggio consentono di identificare una serie di stati o occorrenze identiche. Ad esempio, è possibile applicare una regola che avvisa di cinque o più accessi non riusciti da parte di un account di amministratore. Prima di applicare una regola, è necessario verificare di aver creato le destinazioni di notifica desiderate per il proprio ambiente.

Per selezionare e applicare la regola 5 tentativi di accesso non riuscito per Account amministratore

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria ed espandere la cartella Regole di correlazione.
2. Espandere la cartella Gestione minacce, quindi la cartella Attività account e accesso sospette e selezionare la regola 5 tentativi di accesso non riuscito per Account amministratore.

   I dettagli della regola verranno visualizzati nel riquadro a destra.
3. Rivedere i dettagli della regola per verificare che sia appropriata per il proprio ambiente. In questo caso, i filtri consentono di definire un account amministratore come nome utente appartenente all'elenco con chiave 'Administrators' e di impostare la soglia di conteggio su 5 eventi in 60 minuti.
4. (Facoltativo) Fare clic su Modifica nella parte superiore del riquadro per modificare le impostazioni del filtro, se necessario. Ad esempio, è possibile modificare la soglia temporale in 3 eventi in 30 minuti.

   Viene visualizzata la procedura guidata di gestione delle regole, popolata con i dettagli della regola.

5. Aggiungere i dettagli di notifica desiderati nella procedura guidata. I dettagli di notifica forniscono il contenuto del messaggio che verrà inviato come specificato in Destinazioni di notifica.
6. Dopo aver terminato la preparazione della regola, fare clic su Salva e chiudi. Quando si modifica e si salva una regola di correlazione predefinita, CA User Activity Reporting Module crea automaticamente una nuova versione, preservando la versione originale.
7. Fare clic sulla sottoscheda Servizi e quindi espandere il nodo Servizio di correlazione.
8. Selezionare il server a cui si desidera applicare la regola. Se si dispone di un server identificato come server di correlazione, selezionare tale server.
9. Fare clic su Applica nell'area Configurazione regola, quindi selezionare la nuova versione della regola 5 tentativi di accesso non riuscito per Account amministratore, con la destinazione di notifica che si desidera associare alla regola.
10. Fare clic su OK per chiudere la finestra di dialogo e attivare la regola.

Esempio: selezione e applicazione di una regola di transizione di stato

Le regole di correlazione di transizione di stato consentono di identificare una serie di stati o occorrenze una dopo l'altra. Ad esempio, è possibile applicare una regola che avvisi per una serie di accessi non riusciti seguita da un accesso riuscito da parte dello stesso account utente. Prima di applicare una regola, è necessario verificare di aver creato le destinazioni di notifica desiderate per il proprio ambiente.

1. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Libreria ed espandere la cartella Regole di correlazione.
2. Espandere la cartella Identità, quindi la cartella Autenticazione e selezionare la regola Accessi non riusciti seguiti da accesso corretto.

   I dettagli della regola verranno visualizzati nel riquadro a destra.
3. Rivedere i dettagli della regola per verificare che sia appropriata per il proprio ambiente. In questo caso, nel riquadro Dettagli vengono visualizzati i due stati registrati dalla regola. Il primo è cinque o più accessi non riusciti per lo stesso account utente o identità. Il secondo è un accesso riuscito da parte dello stesso utente o identità.
4. (Facoltativo) Fare clic su Modifica nella parte superiore del riquadro per modificare le impostazioni relative allo stato, se necessario.

   Verrà visualizzata la procedura guidata di gestione delle regole, che mostra i due stati che costituiscono la regola.

5. Fare doppio clic su qualsiasi stato che si desidera modificare.

   Verrà visualizzata la procedura guidata Definizione dello stato, con i dettagli relativi allo stato.

6. Apportare le modifiche desiderate allo stato selezionato, quindi fare clic su Salva e chiudi per tornare alla procedura guidata di gestione delle regole. Ad esempio, il primo stato verifica la presenza di 5 accessi non riusciti in 10 minuti. È possibile modificare la soglia relativa al numero di accessi non riusciti, il tempo o entrambi.

7. Aggiungere i dettagli di notifica desiderati nella procedura guidata. I dettagli di notifica forniscono il contenuto del messaggio che verrà inviato come specificato in Destinazioni di notifica.

8. Dopo aver terminato la preparazione della regola, fare clic su Salva e chiudi. Quando si modifica e si salva una regola di correlazione predefinita, CA User Activity Reporting Module crea automaticamente una nuova versione, preservando la versione originale.

9. Fare clic sulla sottoscheda Servizi e quindi espandere il nodo Servizio di correlazione.

10. Selezionare il server a cui si desidera applicare la regola. Se si dispone di un server identificato come server di correlazione, selezionare tale server.

11. Fare clic su Applica nell'area Configurazione regola, quindi selezionare la nuova versione della regola Accessi non riusciti seguiti da accesso corretto, con la destinazione di notifica desiderata associata alla regola.

12. Fare clic su OK per chiudere la finestra di dialogo e attivare la regola.

Ulteriori informazioni:

Informazioni sulle notifiche di incidente (a pagina 638)
Informazioni sulle regole di correlazione (a pagina 632)
Impostazione di valori predefiniti per la notifica (a pagina 641)

Utilizzo degli elenchi con chiave con le regole di correlazione

Tutte le regole di correlazione vengono generate da uno o più filtri. Alcuni filtri della regola predefiniti sono progettati per selezionare tutti valori di una determinata tabella, in cui un determinato campo di attributo contiene un valore utilizzato come criterio per la compilazione dell'elenco dei valori principali.

È possibile utilizzare gli elenchi con chiave nelle regole di creazione, applicazione o correlazione per fornire valori predefiniti o personalizzati ai filtri della regola. È inoltre possibile aggiornare gli elenchi dei valori con chiave manualmente o automaticamente per mantenere l'elenco aggiornato. Per utilizzare gli elenchi con chiave con le regole di correlazione fare riferimento alla modalità utilizzata per i rapporti.

Per ulteriori informazioni sull'utilizzo degli elenchi con chiave, consultare il capitolo Query e rapporti della presente guida.

Ulteriori informazioni:

Preparazione all'utilizzo di rapporti dotati di elenchi con chiave (a pagina 347)
Approcci alla manutenzione degli elenchi con chiave (a pagina 352)
Creare i valori chiave per i rapporti predefiniti (a pagina 360)

Esempio: creazione di un file CSV per il test

Questo esempio illustra la creazione di un file CSV per il test di una regola di correlazione. È inteso per la verifica di una regola che cerca cinque accessi non riusciti seguiti da un accesso riuscito da parte di un singolo utente.

Per creare un file CSV per il test di una regola per accessi non riusciti seguiti da un accesso riuscito

1. Accedere a CA User Activity Reporting Module come amministratore e fare clic sulla scheda Query e rapporti.
2. Cercare la query "Cinque accessi non riusciti nell'ultima ora per Esecutore".
3. Eseguire la query e visualizzare i risultati. Se sono presenti risultati, andare al passaggio successivo. In caso contrario, creare un utente fittizio, disconnettersi e creare accessi non riusciti utilizzando il nuovo utente fittizio.
4. Esportare la query in formato CSV e aprire il file CSV in Excel.
5. Aggiungere altri dettagli utente come necessario. Ad esempio, aggiungere informazioni relative all'accesso completato con successo.
6. Quando il file CSV contiene tutte le informazioni evento necessarie, salvarlo.
7. Aprire la regola che si desidera sottoporre a test in Esplora libreria, quindi fare clic sulla scheda Test della regola nel riquadro dei dettagli.
8. Caricare il file CSV e verificare che vengano creati gli incidenti corretti.

Informazioni sulle notifiche di incidente

Le notifiche trasmettono informazioni su un incidente. È possibile impostare l'attivazione automatica delle notifiche ogni volta che viene creato un incidente, oppure inviarle manualmente dopo aver visualizzato l'incidente. In entrambi i casi, è innanzitutto necessario definire le destinazioni di notifica da utilizzare nel proprio ambiente.

È necessario creare le notifiche in due parti:

1. Destinazione di notifica, che può contenere qualsiasi combinazione dei tipi di destinazione disponibili. Ad esempio, una destinazione potrebbe contenere indirizzi di posta elettronica, credenziali di server SNMP e un nome di processo IT PAM. Le destinazioni possono essere assegnate a più regole.
2. Dettagli di notifica, che vengono aggiunti alle singole regole e contengono le informazioni inviate dalla notifica, ad esempio oggetto e testo del messaggio di posta elettronica, dati SNMP, parametri di processo IT PAM.

Le notifiche automatiche richiedono una regola di correlazione contenente i dettagli di notifica e una destinazione di notifica associata. Se sono presenti entrambi i componenti, ogni volta che la regola crea un incidente, una notifica automatica viene inviata alle destinazioni specificate. La combinazione di destinazioni e dettagli consente di impostare la notifica modulare. Ad esempio, è possibile inoltrare le stesse informazioni di notifica a service desk regionali diversi o a personale IT diverso.

È inoltre possibile assegnare le destinazioni da incidenti esistenti. Quando si apre un incidente e si assegna una destinazione di notifica, i dettagli di notifica specificati nella regola vengono inviati immediatamente. Per l'invio di notifiche manuali è necessario che la regola includa le notifiche.

Ulteriori informazioni:

Impostazione di valori predefiniti per la notifica (a pagina 641)
Informazioni sulle regole di correlazione (a pagina 632)

Come progettare e applicare le notifiche di incidente

È possibile configurare notifiche per le regole di correlazione. Le notifiche consentono di trasmettere informazioni chiave sugli incidenti rilevati al personale specificato, oppure di creare automaticamente ticket per il service desk CA IT PAM.

Per progettare e configurare le notifiche nel proprio ambiente, attenersi alla seguente procedura:

1. Pianificare e creare le destinazioni di notifica.
2. Selezionare le regole di correlazione predefinite, oppure creare regole personalizzate da utilizzare nel proprio ambiente.
3. Aggiungere dettagli di notifica alle regole per le quali si desidera impostare le notifiche.
4. Applicare le regole di correlazione ai server CA User Activity Reporting Module e assegnare le destinazioni di notifica.

Ulteriori informazioni:

Informazioni sulle regole di correlazione (a pagina 632)
Impostazione di valori predefiniti per la notifica (a pagina 641)
Considerazioni sul servizio di correlazione (a pagina 158)

Impostazione di valori predefiniti per la notifica

È possibile impostare i dettagli di notifica in una regola, specificando in tal modo il contenuto della notifica, ma non le destinazioni. Ad esempio, è possibile impostare l'oggetto e il contenuto di un messaggio di posta elettronica, ma non gli indirizzi di recapito, che sono controllati dalle destinazioni di notifica. Il sistema consente di impostare contenuto standard (utilizzando i dettagli), che può essere recapitato a vari destinatari (utilizzando le destinazioni).

Nei dettagli di notifica di una singola regola è possibile includere qualsiasi combinazione dei tipi di notifica disponibili.

Per impostare i dettagli di notifica

1. Aprire la procedura guidata delle regole di correlazione, immettere le definizioni della regola desiderate e procedere al passaggio Dettagli notifica.
2. Per aggiungere le informazioni di notifica di posta elettronica, selezionare la scheda Posta elettronica e attenersi alla seguente procedura:
   a. Immettere un oggetto per la notifica di posta elettronica.
   b. (Facoltativo) Durante l'immissione di testo in qualsiasi campo della scheda Posta elettronica è possibile utilizzare l'elenco a discesa Campi dati e il pulsante Aggiungi per inserire variabili di campo dati. Ad esempio, è possibile scegliere agent_address e fare clic su Aggiungi.

      "%agent_address%" viene visualizzato nel campo di testo. Quando una regola genera un messaggio di posta elettronica, il valore del campo agent_address viene visualizzato in sostituzione della variabile.
   c. Immettere il corpo del messaggio di posta elettronica di notifica.

      Nota: il corpo del messaggio è in formato HTML, pertanto il testo inserito verrà visualizzato su un'unica riga. Per creare un'interruzione dopo una riga, inserire <BR/> alla fine della riga di testo.
3. Selezionare la scheda Processo e attenersi alla seguente procedura per aggiungere parametri di processo CA IT PAM:
   a. Immettere il nome del processo IT PAM al quale si desidera passare le informazioni di incidente, ad esempio:
      `/CA_ELM/EventAlertOutput`
   b. Fare clic su Aggiungi parametro per specificare un parametro e il relativo valore.

      Verrà visualizzata la finestra di dialogo Aggiungi parametro di processo.
   c. Digitare un nome di parametro nel campo Nome, ad esempio 'Gravità'.

d. Definire un valore digitandolo nell'area del valore oppure selezionando un campo CEG dall'elenco a discesa e quindi facendo clic su Aggiungi campo dati. Le informazioni evento specificate tramite il campo CEG vengono passate al parametro denominato. Continuando l'esempio del passaggio precedente, è possibile selezionare 'event_severity' per presentare il valore del campo event_severity come parametro Gravità di IT PAM.

e. Ripetere i passaggi a-c per aggiungere ulteriori parametri e valori come necessario.

f. Dopo aver aggiunto tutti i campi CEG desiderati per il parametro corrente, fare clic su OK.

   Nota: per definire un parametro è possibile digitare e aggiungere più campi CEG, in base alle proprie esigenze. Se ad esempio si desidera definire il parametro Descrizione per una notifica utilizzata con una regola di individuazione account, è possibile inserire:

   ```
   Questo incidente segnala quattro tentativi di accesso non riusciti da
   %dest_identity_unique_name% su %dest_hostname% avvenuti in 10 minuti.
   ```

   La struttura *%value%* è il risultato della selezione di un campo CEG e dell'utilizzo del pulsante Aggiungi campo dati, come descritto nel passaggio b.

4. Per aggiungere le impostazioni dei trap SNMP, selezionare la scheda SNMP e attenersi alla seguente procedura:
   a. Modificare l'ID trap personalizzato come richiesto per la destinazione della trasmissione SNMP.
   b. Immettere il nome di un campo CEG che si desidera inviare nell'area di immissione. La digitazione all'interno del campo restringe le scelte disponibili nell'elenco a discesa.
   c. Fare clic su Aggiungi.
   d. Il nome del campo CEG viene visualizzato nell'area dei campi selezionati. Le informazioni evento presenti in questo campo vengono inviate per le regole che utilizzano questo modello di notifica. È necessario specificare almeno un campo CEG.
   e. Ripetere i passaggi b-c per inviare ulteriori campi CEG.
5. Fare clic sulla freccia appropriata per andare al passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Se si fa clic su Salva e chiudi, la nuova regola verrà visualizzata nella cartella appropriata. In alternativa, verrà visualizzato il passaggio selezionato.

Ulteriori informazioni:

Informazioni sulle regole di correlazione (a pagina 632)
Informazioni sulle notifiche di incidente (a pagina 638)

Capitolo 19: Attività di gestione incidenti

Un incidente CA User Activity Reporting Module è composto da uno o più eventi, identificati e collegati da una regola di correlazione. Ogni volta che una regola di correlazione regola rileva uno o più eventi che soddisfano i criteri, CA User Activity Reporting Module crea un incidente.

Se si dispone del ruolo di amministratore, è possibile eseguire le seguenti attività di gestione incidente:

- Visualizzare i dettagli relativi agli incidenti creati dalle regole di correlazione nel proprio ambiente.
- Filtrare l'elenco incidenti o impostare le condizioni di risultato per individuare particolari incidenti o tipi di incidenti, oppure restringere la visualizzazione incidenti.
- Applicare destinazioni di notifica agli incidenti esistenti, controllando le risposte quali una notifica tramite posta elettronica.
- Esportare le informazioni su un incidente.
- Pianificare gli avvisi basati su un incidente.
- Unire gli incidenti esistenti in un nuovo incidente.

Nota: per ulteriori informazioni sulle attività di gestione degli incidenti consultare la *Guida in linea di CA User Activity Reporting Module.*

Visualizzazione di dettagli su un incidente

È possibile visualizzare i dettagli relativi agli incidenti nel proprio ambiente, con informazioni sullo stato, la priorità e la cronologia. È possibile visualizzare soltanto gli eventi che vengono inoltrati al server di correlazione in cui è stato eseguito l'accesso. È possibile controllare il modo in cui il server CA User Activity Reporting Module inoltra gli eventi configurando il Servizio di correlazione.

Per visualizzare i dettagli sugli incidenti

1. Fare clic sulla scheda Incidenti, selezionare l'incidente che si desidera esaminare e fare doppio clic sulla riga dell'incidente.

   Verrà visualizzata la finestra di dialogo Dettagli, in cui vengono mostrati i dettagli di base sull'incidente, tra cui nome, data e gravità.

2. Modificare le impostazioni Priorità o Stato utilizzando i menu a discesa appropriati.
3. (Facoltativo) Fare clic sulla scheda Cronologia per visualizzare informazioni quali il numero e l'ora degli eventi aggiunti all'incidente o le notifiche automatiche attivate.
4. Fare clic su OK o Applica.

Ulteriori informazioni:

Considerazioni sul servizio di correlazione (a pagina 158)

Capitolo 20: Attività dei profili di raccolta evento

Questa sezione contiene i seguenti argomenti:

Creazione di un profilo di raccolta evento (a pagina 647)
Impostazione delle informazioni relative al profilo di raccolta (a pagina 648)
Applicazione delle regole di soppressione e riepilogo (a pagina 649)
Configurazione del profilo di raccolta (a pagina 650)

Creazione di un profilo di raccolta evento

Un profilo di raccolta evento contiene le informazioni basiche necessarie per la creazione di un listener o un connettore CA User Activity Reporting Module. In tal modo è possibile applicare il provisioning della raccolta eventi quando l'API di automatizzazione virtuale chiama il profilo.

Prima di poter utilizzare l'API virtuale è necessario creare profili di raccolta. Ciascun profilo di raccolta conterrà le informazioni relative a un'integrazione o un listener specifici. Si consiglia pertanto di creare più profili di raccolta adatti al proprio ambiente. Per poter creare, modificare o gestire profili di raccolta è necessario disporre del ruolo di amministratore.

Per ulteriori informazioni sulle impostazioni dei connettori e dei listener, consultare la Guida in linea o la Guida al connettore relative al tipo di evento che si desidera raccogliere.

Le seguenti fasi consentono la creazione di un profilo di raccolta eventi:

1. Impostazione delle informazioni relative al profilo di raccolta
2. Applicazione delle regole di soppressione
3. Applicazione di regole di riepilogo
4. Configurazione del profilo di raccolta.

Ulteriori informazioni:

Impostazione delle informazioni relative al profilo di raccolta (a pagina 648)
Configurazione del profilo di raccolta (a pagina 650)

Impostazione delle informazioni relative al profilo di raccolta

Per avviare la creazione del profilo di raccolta, definire le informazioni di identificazione del profilo, quindi specificare il tipo di evento di raccolta.

Procedere come descritto di seguito:

1. Fare clic sulla scheda Amministrazione, selezionare scheda secondaria Libreria, quindi la cartella Profili di raccolta evento.
2. Fare clic su Nuovo profilo di raccolta

   Verrà visualizzata la procedura guidata del profilo di raccolta.
3. Immettere un nome e una descrizione per il profilo.
4. Selezionare il gruppo agenti che si desidera associare al profilo. CA User Activity Reporting Module utilizza un agente del gruppo selezionato per eseguire la distribuzione della raccolta di eventi.
5. Selezionare integrazioni o listener in base al metodo di raccolta desiderato per il profilo.
6. Se si selezionano le integrazioni, scegliere l'integrazione desiderata dall'elenco a discesa.
7. Se si selezionano i listener, scegliere il listener e l'integrazione desiderati dall'elenco a discesa.
8. Selezionare l'operazione che si desidera eseguire.

Applicazione delle regole di soppressione e riepilogo

Un profilo eventi consente l'applicazione sia di regole di soppressione che di aggregazione. Durante la distribuzione del profilo eventi, le regole di soppressione e di aggregazione selezionate verranno applicate a livello di agente. Il controllo di soppressione e riepilogo va ad aggiungersi al controllo analogo eseguito nel deposito eventi di log.

Importante: Creare e utilizzare le regole di soppressione con cautela perché impediscono la registrazione e la visualizzazione completa di determinati eventi nativi. È consigliabile verificare le regole di soppressione in un ambiente di prova prima di distribuirle.

Per applicare le regole di soppressione e riepilogo:

1. Aprire la procedura guidata di progettazione del profilo di raccolta ed accedere alla fase Regole di soppressione o Regole di riepilogo.
2. (Facoltativo) Digitare nel campo del modello delle regole per ricercare le regole disponibili. Mentre si digita vengono visualizzare le regole che corrispondono a quanto immesso.
3. Selezionare le regole desiderate utilizzando il controllo pilota.
4. Fare clic sulla freccia appropriata per andare al passaggio della procedura guidata che si desidera completare successivamente, oppure fare clic su Salva e chiudi.

   Facendo clic su Salva e chiudi, il nuovo profilo verrà visualizzato nell'elenco della cartella Utente. In caso contrario, verranno visualizzate le operazioni selezionate.

Configurazione del profilo di raccolta

Configurare il profilo di raccolta eventi aggiungendo le informazioni richieste in modo che CA User Activity Reporting Module ricerchi le informazioni a partire dall'origine specificata.

Per configurare il profilo di raccolta:

1. Aprire la procedura guidata del profilo di raccolta, immettere le informazioni richieste e passare alla fase di configurazione.

   Verranno visualizzate le operazioni di configurazione, contenenti i parametri del sensore per il connettore o il tipo di listener impostato nella fase 1.

2. Immettere i dettagli di configurazione richiesti. Consultare la Guida al connettore corrispondente per ulteriori informazioni su valori di campo specifici. Per alcune configurazioni verrà visualizzato un elenco delle chiavi di input. È possibile selezionare e trascinare chiavi di input per impostare una variabile per determinati campi di immissione. Ad esempio è possibile trascinare la chiave ID utente in un campo Nome utente. La chiave verrà visualizzata in formato %ID utente %, consentendo al profilo eventi di individuare in modo automatico la stringa specificata durante la distribuzione.

   Nota: le chiavi di input sono richieste per il funzionamento dei metodi API GET e PUT. Utilizzare qualsiasi chiave di input disponibile per il tipo di connessione utilizzata anziché digitare i valori direttamente nei campi di immissione.

3. Se l'accesso all'origine dell'evento richiede un nome utente e una password, selezionare Credenziali obbligatorie. Si tratta solitamente di connettori attivi come WinRM.

4. Fare clic su Salva e chiudi.

Capitolo 21: Agenti

Questa sezione contiene i seguenti argomenti:

Pianificazione dell'installazione di un agente (a pagina 651)
Pianificazione della configurazione degli agenti (a pagina 654)
Attività di gestione agente (a pagina 660)
Aggiornamento della Chiave di autenticazione agente (a pagina 661)
Download dei file binari agente (a pagina 662)
Configurazione di un agente (a pagina 662)
Visualizzare il dashboard di agente (a pagina 666)
Visualizzazione e controllo dello stato di agenti o connettori (a pagina 667)
Modalità di creazione di un gruppo di agenti (a pagina 669)
Modalità di configurazione della gestione agente (a pagina 672)
Modalità di protezione degli agenti dalle conseguenze dei cambi di indirizzo IP dei server (a pagina 676)
Modalità di applicazione degli aggiornamenti di sottoscrizione (a pagina 679)
Creazione di un file di diagnosi agente per il Supporto (a pagina 683)

Pianificazione dell'installazione di un agente

Al momento di pianificare l'installazione degli agenti, il responsabile deve determinare quanti agenti sono necessari e dove installarli. Questa pianificazione può essere eseguita dall'utente incaricato dell'installazione degli agenti, da un amministratore di rete o da un architetto di sistema.

Per pianificare le installazioni degli agenti

1. Creare una versione elettronica della tabella di pianificazione per l'installazione degli agenti idonea per la registrazione delle informazioni necessarie. Si consiglia di utilizzare la seguente tabella e le intestazioni di colonna di esempio riportate di seguito.

Piattaforma origine evento	Nome host o indirizzo IP utilizzati dall'origine evento	Uno dei seguenti elementi: - Senza agente-Diretto - Senza agente-Punto di raccolta - Agente sull'endpoint	Nome host o indirizzo IP dove deve essere installato l'agente

2. Identificare ogni origine evento da destinare alla raccolta registri e registrarne la posizione e la piattaforma nella tabella di pianificazione degli agenti.

3. Valutare i costi e i vantaggi di ogni tipo di soluzione.

	Vantaggio	Svantaggio o limitazione
Senza agente - Diretto da CA User Activity Reporting Module - Nessun agente installato	Non è richiesta l'installazione di agenti.	Si può eseguire la raccolta solo delle origini evento compatibili con la piattaforma di applicazione software. Costi della soluzione senza agente - Si applicano anche i punti di raccolta.
Senza agente - Agente sul punto di raccolta	Non occorre installare agenti sull'host sul quale è in funzione l'origine evento. Il consolidamento della raccolta in un unico punto riduce il numero di agenti che occorre installare rispetto alle raccolte basate sugli agenti.	Le regole di soppressione possono essere applicate soltanto sul server CA User Activity Reporting Module e non è possibile sfruttare la riduzione del traffico di rete. La comunicazione degli eventi tra l'origine e il server CA User Activity Reporting Module non è crittografata. L'origine evento deve essere in grado di eseguire l'accesso da remoto.
Basato su agente - Agente sull'end-point	È possibile applicare le regole di soppressione all'origine invece che sul server CA User Activity Reporting Module. Questo riduce il traffico di rete tra il punto di raccolta e il server CA User Activity Reporting Module. La comunicazione dei registri tra l'origine e il server CA User Activity Reporting Module è crittografata. Delle tre soluzioni, questa è quella che può ospitare il maggior volume di eventi.	Un agente deve essere installato dove è in funzione l'origine evento.

4. Registrare la soluzione preferita per ogni origine evento.
5. Ordinare la tabella di pianificazione degli agenti per la colonna 3 e poi per la 2. In questo modo vengono visualizzate tutte le origini evento basate su agente in esecuzione in blocchi sullo stesso host.

6. Per le origini evento mappate come basate sugli agenti, trovare la prima occorrenza in un blocco con lo stesso nome e copiare i dati dalla colonna 2 alla 4. In questo modo si ottiene una sola voce per ogni host su cui sono in funzione una o più origini evento (non occorre mai più di un agente su un dato host, a prescindere dal numero di origini evento).
7. Per le origini evento mappate come senza agente-punto di raccolta, utilizzare il seguente metodo per pianificare la posizione di installazione degli agenti:
   a. Identificare il numero di punti di raccolta necessari per ospitare le origini evento identificate come candidate per gli agenti remoti.
   b. Pianificare il raggruppamento di origini evento identificate come candidate per gli agenti remoti in base a un'area comune di posizione sulla rete.
   c. Per ogni gruppo di origine evento, identificare il server da utilizzare come punto di raccolta. Può essere un server dedicato. Registrare la propria decisione nella colonna 4.
8. Se si utilizza un adattatore CA obsoleto e vengono registrate origini evento per cui non esistono soluzioni mappate e si desiderano ulteriori informazioni, consultare la *Guida all'implementazione di CA User Activity Reporting Module*.
9. Trasmettere i dati registrati nella quarta colonna della tabella di pianificazione dell'agente all'utente incaricato dell'installazione degli agenti.

Pianificazione della configurazione degli agenti

L'utente EiamAdmin installa gli agenti scegliendo il miglior metodo di raccolta. Sono disponibili i seguenti metodi:

- Raccolta registri senza agente direttamente dal server CA User Activity Reporting Module, talvolta denominata raccolta diretta.
- Raccolta registri senza agente da un punto di raccolta
- Raccolta registri basata su agente dall'host in cui è in esecuzione l'origine evento

L'analisi che precede l'installazione può rilevare informazioni necessarie all'amministratore che configura agenti e connettori.

Il primo passaggio nella configurazione degli agenti prevede di ottenere il foglio di calcolo relativo alla pianificazione degli agenti dall'EiamAdmin, oppure quello alternativo utilizzato per documentare la posizione in cui sono installati gli agenti. Una volta configurato il primo amministratore, l'utente EiamAdmin fornisce all'amministratore il foglio di lavoro di pianificazione dell'installazione dell'agente. Il primo amministratore, a sua volta, pianifica i connettori necessari per ogni agente prima di iniziare la configurazione.

L'amministratore configura tutti gli agenti installati dall'EiamAdmin. Inoltre, l'amministratore configura un connettore per ogni origine evento, indipendentemente dal metodo di raccolta (senza agente -diretto, senza agente-con punto di raccolta o basato su agente). L'amministratore configura i connettori su ogni agente restando connesso al server CA User Activity Reporting Module destinato alla ricezione degli eventi raccolti da tale agente.

Nota: meno connettori vengono configurati su un agente, migliori sono le prestazioni.

Un'eccezione a questo processo si verifica quando l'installazione degli agenti viene eseguita in modo invisibile. In questo caso, è il programma di installazione a configurare i connettori. I connettori configurati su un agente lo attivano, permettendogli di raccogliere eventi non elaborati da origini evento specifiche. I connettori trasformano gli eventi non elaborati in eventi perfezionati e li trasmettono poi a CA User Activity Reporting Module.

La creazione di gruppi di agenti è facoltativa. Se non viene creato nessun gruppo di agenti, gli agenti saranno assegnati al gruppo agenti predefinito. Gli amministratori creano gruppi di agenti per le seguenti ragioni:

- Per abilitare la creazione di report di eventi raccolti dagli agenti nello stesso gruppo di agenti.
- Per abilitare l'assegnazione di un utente amministrativo diverso a diversi gruppi di agenti (l'accesso degli utenti può essere limitato a un gruppo di agenti specificato con criteri di accesso).

I registri eventi raccolti vengono inviati al server CA User Activity Reporting Module per l'elaborazione e l'archiviazione iniziale. Gli amministratori devono configurare il server che riceverà i registri per ogni agente o gruppo di agenti. L'assegnazione di un server a un gruppo di agenti è un modo rapido per assegnare il server a tutti gli agenti del gruppo di agenti.

Pianificazione della raccolta registri diretta

CA User Activity Reporting Module viene installato con un agente predefinito che può essere utilizzato per la raccolta registri diretta. Viene chiamata raccolta diretta in quanto l'utilizzo dell'agente predefinito non richiede l'installazione di altri agenti. L'agente predefinito può raccogliere eventi quasi da ogni origine evento, con le limitazioni elencate di seguito.

- Il sensore di registro deve poter funzionare sull'applicazione software; alcuni sensori di registro, come il WMI, sono legati a una piattaforma specifica.
- L'origine evento deve essere in grado di eseguire l'accesso da remoto.

L'agente predefinito viene configurato proprio come si configurerebbe un agente installato separatamente. La raccolta registri diretta tramite l'agente predefinito è ideale per i sistemi più piccoli.

Origini eventi per Raccolta registro diretta

CA User Activity Reporting Module fornisce sensori di registro che possono essere eseguiti sul server CA User Activity Reporting Module per semplificare la raccolta registro diretta senza agenti. Al momento della pubblicazione del presente documento, sono supportati:

- syslog
- WinRM
- ODBC
- TIBCO

Per determinare le integrazioni supportate dall'agente predefinito

1. Selezionare un server CA User Activity Reporting Module da Explorer agente, nella sottoscheda Raccolta registro della scheda Amministrazione.
2. Fare clic su Crea nuovo connettore.

L'elenco a discesa Integrazione include le integrazioni dalle quali è possibile creare un connettore per la distribuzione sull'agente predefinito. Ciascuna integrazione su cui sono basati i connettori ha lo scopo di recuperare eventi da una specifica origine eventi.

Per un elenco completo di integrazioni e sensori di registro supportati, consultare la pagina di prodotto CA User Activity Reporting Module nell'area Assistenza clienti.

Un **sensore di registro** è un componente di integrazione progettato per leggere uno specifico tipo di registro, come database, syslog, file o SNMP.

Pianificazione della raccolta registri priva di agenti

La raccolta registri priva di agenti può essere implementata con l'installazione di un agente su un server di raccolta che raccolga eventi da più origini evento remote.

Al momento di pianificare la configurazione della raccolta registri priva di agenti da un server di raccolta, è opportuno tenere presente quanto segue:

- Meno connettori vengono distribuiti a un agente, migliori sono le prestazioni.
- Il numero massimo di connettori da configurare su un determinato agente dipende da diversi fattori: se l'agente è installato su un server dedicato, quanto è potente questo server e che tipo di origini evento sono considerate. In linea di massima, non si dovrebbero configurare più di quaranta o cinquanta connettori su un singolo agente.
- Non si ottiene alcun vantaggio nelle prestazioni se si raggruppano i connettori dello stesso tipo configurati su agenti diversi nello stesso server di raccolta. Di conseguenza, non si ottiene alcun vantaggio nelle prestazioni nemmeno se si dirigono gli eventi dallo stesso tipo di origine evento a uno specifico server CA User Activity Reporting Module in una federazione.

Pianificazione della raccolta di registri basata sugli agenti

Dopo l'installazione di un agente su un server con origini evento locali, su quell'agente gli amministratori configurano un connettore per ogni origine evento funzionante a livello locale.

Se sono presenti molti server di destinazione con gli stessi tipi di origine evento, è consigliabile raggruppare tali server in un gruppo di agenti ed eseguire la configurazione a livello di tale gruppo.

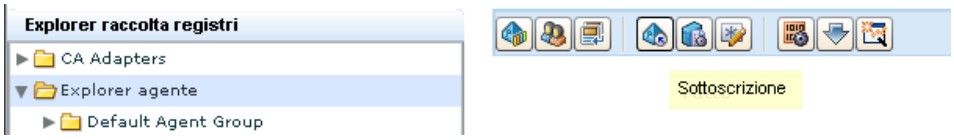
La garanzia di recapito può rivelarsi un problema per la raccolta diretta dei syslog. Per evitarlo, configurare un listener syslog su un agente installato con l'origine evento syslog.

Selezione del livello da configurare

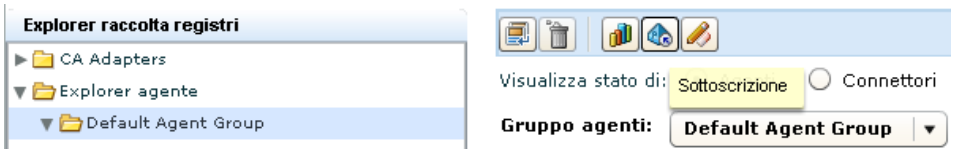
Le opzioni Sottoscrizione, Applica regole di soppressione e Stato possono essere selezionate da diversi livelli. Ad esempio, la configurazione di sottoscrizione si può avviare dai seguenti livelli:

- Explorer agente
- Gruppo agenti predefinito oppure gruppo di agenti definito dall'utente
- Agente

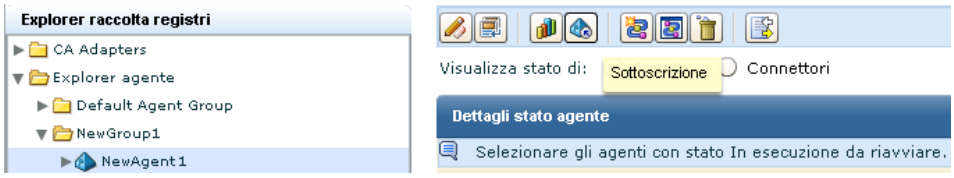
Per configurare un'opzione in modo da poterla applicare a tutti gli agenti di ogni gruppo, selezionare Explorer agente e quindi fare clic sul pulsante relativo all'azione da eseguire.



Per configurare un'opzione in modo da poterla applicare a tutti gli agenti di un gruppo selezionato, selezionare il nome del gruppo e fare clic sul pulsante relativo all'azione da eseguire.



Per configurare un'opzione in modo da poterla applicare ad un solo agente, selezionare l'agente e fare clic sul pulsante relativo all'azione da eseguire.



Attività di gestione agente

Explorer agente consente di visualizzare e di gestire gli agenti di raccolta degli eventi nel proprio ambiente. È possibile utilizzare l'interfaccia di Explorer agente per eseguire operazioni di gestione nelle seguenti aree:

- Configurazione agente: consente di rinominare gli agenti e di configurare i gruppi a cui essi appartengono, e quelli a loro associati.
- Gruppi agente: consente di raggruppare gli agenti, ad esempio, in base alla zona geografica, all'importanza aziendale o al tipo di origine evento. Se necessario, è possibile anche assegnare agenti raggruppati a diversi server CA User Activity Reporting Module.
- Sottoscrizioni: consentono di visualizzare gli aggiornamenti disponibili e di applicarli agli agenti.
- Comando e stato agente: consente di visualizzare lo stato attuale degli agenti, e di arrestarli e riavviarli se necessario.

Ulteriori informazioni

Download dei file binari agente (a pagina 662)
Aggiornamento della Chiave di autenticazione agente (a pagina 661)
Modalità di creazione di un gruppo di agenti (a pagina 669)
Modalità di applicazione degli aggiornamenti di sottoscrizione (a pagina 679)
Modalità di configurazione della gestione agente (a pagina 672)

Aggiornamento della Chiave di autenticazione agente

È possibile visualizzare ed aggiornare la chiave utilizzata dagli agenti per registrarsi con il server CA User Activity Reporting Module. Modificando questa chiave regolarmente sarà possibile impedire l'installazione di agenti non autorizzati nel proprio ambiente. Per impostazione predefinita, si utilizza la stessa chiave su tutte le istanze di applicazione di tutti i server CA User Activity Reporting Module. Tuttavia, è possibile impostare questa chiave in modo che sia univoca per ogni istanza applicazione.

L'installatore dell'agente deve inserire questa chiave come codice di autorizzazione nella procedura guidata di installazione dell'agente.

Per aggiornare la chiave di autenticazione agente

1. Fare clic sulla scheda Amministrazione e quindi sulla sottoscheda Raccolta registri.

   Apparirà l'elenco della cartella Raccolta registri.

2. Fare clic sulla cartella Explorer agente.

   Nel riquadro dei dettagli verranno visualizzati i pulsanti relativi alla gestione agenti.

3. Fare clic su Chiave di autenticazione agente:

   Verrà visualizzato il pannello Chiave di autenticazione agente.

4. Digitare una nuova chiave nei campi Immettere chiave e Confermare chiave, e fare clic su Salva.

   Verrà visualizzato un messaggio di conferma dell'avvenuta operazione.

Download dei file binari agente

È possibile scaricare i file binari agente ed installarli sul computer locale senza utilizzare altri supporti di installazione.

Per ulteriori informazioni sull'installazione degli agenti, consultare la *Guida all'installazione degli agenti CA User Activity Reporting Module*.

Per scaricare i file binari agente

1. Fare clic sulla scheda Amministrazione, e quindi sulla sottoscheda Raccolta registri.

   Verrà visualizzato l'elenco cartella di Raccolta registri.

2. Fare clic sulla cartella Explorer agente.

   Nel riquadro dei dettagli vengono visualizzati i pulsanti di gestione agente.

3. Fare clic su Download file binari agente:

   Verrà visualizzato l'Elenco file binari agente, che contiene gli agenti disponibili e la loro versione attuale.

4. Fare clic sull'agente da scaricare.

   Verrà visualizzata una finestra di dialogo per scaricare i file.

5. Scegliere il percorso in cui salvare il file binario agente e fare clic su Salva.

   Il file sarà salvato nella posizione scelta, ed apparirà un messaggio di conferma.

Configurazione di un agente

È possibile configurare un agente installato e registrato solo a patto di accedervi con Explorer agente.

Per configurare un agente

1. Fare clic sulla scheda Amministrazione, e quindi sulla sottoscheda Raccolta log.

   Verrà visualizzato l'elenco cartella di Raccolta log.

2. Fare clic sulla cartella Explorer agente.

   La cartella si espande e mostra le cartelle Gruppo di agenti.

3. Selezionare l'agente da configurare e fare clic su Modifica, nella parte superiore del pannello.

I dettagli dell'agente verranno visualizzati nel riquadro dei dettagli.

4. Eseguire le modifiche desiderate, fra cui:

Nome utente

Definisce il nome utente con cui si esegue l'agente.

Porta

Imposta la porta utilizzata dall'agente per comunicare con CA User Activity Reporting Module.

Gruppo agenti

Definisce il gruppo di appartenenza dell'agente.

Numero massimo di file

Consente di impostare il numero massimo di file che possono essere creati nella coda di file di ricezione degli eventi. Il numero massimo consentito corrisponde a 1000 file.

Dimensioni massime per file

Consente di impostare la dimensione massima (in MB) per ciascun file nella coda di file di ricezione degli eventi. Quando un file raggiunge la dimensione massima, CA User Activity Reporting Module crea un nuovo file. La dimensione massima consentita è 2048 MB.

Modalità di invio evento

Definisce quale delle seguenti modalità di trasmissione è utilizzata dall'agente:

- Failover: l'agente invia gli eventi al primo server dell'elenco Server Log Manager. Se la comunicazione viene persa, l'agente tenta di comunicare con il server successivo contenuto nell'elenco, fino al ripristino della comunicazione.
- Round Robin: l'agente invia gli eventi a ciascun server dell'elenco Server Log Manager e tenta di contattare il server successivo dell'elenco con un intervallo di un'ora. Non è possibile configurare questo intervallo.

Attiva la crittografia eventi

Definisce l'agente che utilizza AES128 per eseguire la crittografia della trasmissione eventi. L'abilitazione della crittografia eventi può ridurre le prestazioni.

Attiva pianificazione invio

Definisce l'agente per l'invio degli eventi solo durante un determinato intervallo di tempo. Selezionare la casella di controllo Attiva pianificazione invio per visualizzare i campi Ora di inizio e Ora di fine. Immettere i valori di ora GMT desiderati in formato 24 ore rispettando le seguenti indicazioni:

- Tra l'ora di inizio e l'ora di fine deve esistere un intervallo di un'ora.
- Se l'ora di inizio è successiva all'ora di fine, il valore dell'ora di fine viene impostato per il giorno successivo. Ad esempio, se l'ora di inizio viene impostata alle ore 23 e l'ora di fine alle ore 6, l'intervallo di trasmissione ha inizio alle 23 GMT e finisce alle 6 GMT del giorno successivo.

Sostituisci indirizzo IP con nome host

Imposta l'agente per la sostituzione dell'indirizzo IP di un'origine evento con il nome host dell'origine evento. Tutti i connettori dell'agente ereditano questa funzionalità. Se si desidera abilitare questa funzionalità per tutti gli agenti dell'ambiente in uso, è necessario configurare ciascun agente individualmente. Se questa funzionalità viene abilitata, CA User Activity Reporting Module sostituisce l'indirizzo IP con il nome host nei seguenti campi CEG:

- source_hostname
- dest_hostname
- agent_hostname
- event_source_hostname
- receiver_hostname

Server Log Manager

Controlla i server CA User Activity Reporting Module a cui l'agente indirizza gli eventi, e l'ordine in cui vengono contattati. È possibile utilizzare il controllo pilota per selezionare i server disponibili, e i pulsanti freccia, che si trovano a sinistra dei server selezionati, per impostare la priorità di comunicazione.

Nota: aggiornare i propri server CA User Activity Reporting Module prima di eseguire tale operazione sugli agenti. I server CA User Activity Reporting Module supportano gli agenti della loro stessa versione o di quelle inferiori. Per assicurare una corretta archiviazione degli eventi raccolti quando si configurano o si aggiornano agenti, verificare che l'agente invii eventi solo a server CA User Activity Reporting Module, il cui livello è uguale o superiore a quello dell'agente.

5. Fare clic su Salva.

Ulteriori informazioni

Modalità di creazione di un gruppo di agenti (a pagina 669)

Gestione di un file di configurazione manomesso

Gli agenti utilizzano un file di configurazione archiviato nella memoria quando sono in esecuzione. Se qualcuno manomette un file di configurazione mentre l'agente è in esecuzione, l'agente non utilizza il file manomesso. Quando un agente riceve una nuova configurazione dal server CA User Activity Reporting Module, sostituisce il file su disco con il file ricevuto prima del riavvio. In questo modo, un file manomesso viene automaticamente sostituito con il file corretto.

Se qualcuno riavvia l'agente da un'origine esterna dopo aver manomesso il file, l'Agente rileva che il file è manomesso e si arresta. L'agente non accetta alcun dato di configurazione, tantomeno dall'elenco server CA User Activity Reporting Module del file manomesso.

L'Explorer agente indica che l'agente "non risponde". Utilizzare lo stato del server CA User Activity Reporting Module e gli strumenti di comando per reimpostare la configurazione dell'agente. Dopo questa azione, l'agente riprende a funzionare correttamente.

Visualizzare il dashboard di agente

È possibile visualizzare il dashboard di agente per visualizzare lo stato degli agenti nell'ambiente. Il dashboard visualizza inoltre alcuni dettagli come la modalità FIPS corrente (FIPS o non FIPS), e i dettagli di utilizzo. Questi includono il caricamento eventi al secondo, l'uso percentuale della CPU e la data e l'ora dell'ultimo aggiornamento.

Per visualizzare il dashboard di agente

1. Fare clic sulla scheda Amministrazione, e quindi sulla sottoscheda Raccolta registri.

   Verrà visualizzato l'elenco cartella di Raccolta registri.

2. Selezionare la cartella Explorer agente.

   Nel riquadro dei dettagli vengono visualizzati i pulsanti di gestione agente.

3. Fare clic su Monitoraggio di stato e dashboard di agente:

   Verrà visualizzato il riquadro di ricerca agente, che mostra lo stato di tutti gli agenti disponibili per mezzo di un grafico informativo. Ad esempio:

   `Totale: 10 In esecuzione: 8 In sospeso: 1 Terminati: 1 Non risponde: 0`

4. (Facoltativo) Selezionare i criteri di ricerca degli agenti per restringere l'elenco degli agenti visualizzati. È possibile selezionare uno o più criteri fra i seguenti:

   - Gruppo di agenti: restituisce solo gli agenti assegnati al gruppo selezionato.
   - Piattaforma: restituisce solo gli agenti in esecuzione sulla piattaforma selezionata.
   - Stato: restituisce solo gli agenti con lo stato selezionato, ad esempio In esecuzione.
   - Modello nome agente: restituisce solo gli agenti contenenti il modello specificato.

5. Fare clic su Mostra stato.

   Verrà visualizzato un elenco degli agenti che soddisfano i criteri di ricerca, con l'aggiunta di una serie di informazioni fra cui:

   - Nome e versione del connettore locale
   - Server CA User Activity Reporting Module corrente
   - Modalità FIPS dell'agente (FIPS o non FIPS)
   - Ultimo carico di eventi al secondo registrato e gestito dall'agente
   - Ultimo valore di utilizzo della CPU registrato
   - Ultimo valore di utilizzo della memoria registrato
   - Ultimo aggiornamento di configurazione
   - Stato dell'aggiornamento di configurazione

Visualizzazione e controllo dello stato di agenti o connettori

È possibile monitorare lo stato degli agenti o dei connettori nell'ambiente, riavviare agenti e avviare, terminare e riavviare i connettori secondo le esigenze.

È possibile visualizzare agenti o connettori da livelli diversi della gerarchia della cartella Gestione agenti. Ogni livello restringerà di conseguenza la visualizzazione disponibile:

- Dalla cartella Gestione agenti è possibile visualizzare tutti gli agenti o i connettori assegnati al server CA User Activity Reporting Module corrente.
- Dalla cartella di uno specifico gruppo di agenti è possibile visualizzare gli eventi ed i connettori assegnati a tale gruppo agenti.
- Da un singolo agente è possibile visualizzare solo l'agente in questione ed i connettori ad esso assegnati.

La modalità FIPS (FIPS o non FIPS) per un agente può essere impostata da tutti e tre i livelli.

Per visualizzare lo stato degli agenti o dei connettori

1. Fare clic sulla scheda Amministrazione, e quindi sulla sottoscheda Raccolta log.

   Verrà visualizzato l'elenco cartella di Raccolta log.

2. Selezionare la cartella Gestione agente.

   Nel riquadro dei dettagli vengono visualizzati i pulsanti di gestione agente.

3. Fare clic su Stato e comando:

   Viene visualizzato il riquadro dello stato.

4. Selezionare Agenti o connettori.

   Comparirà il riquadro della ricerca degli agenti o connettori.

5. (Facoltativo) Selezionare i criteri di ricerca degli aggiornamenti degli agenti o dei connettori. Se non vengono immessi termini di ricerca, compariranno tutti gli aggiornamenti disponibili. Per restringere la propria ricerca, è possibile selezionare uno o più criteri fra i seguenti:

   - Gruppo agenti: restituisce solo gli agenti ed i connettori assegnati al gruppo selezionato.
   - Piattaforma: restituisce solo gli agenti ed i connettori in esecuzione sul sistema operativo selezionato.
   - Modello nome agente: restituisce solo gli agenti e i connettori contenenti il modello specificato.
   - (Solo connettori) Integrazione: restituisce solo i connettori utilizzando l'integrazione selezionata.

6. Fare clic su Mostra stato.

   Verrà visualizzato un grafico dei dettagli, che visualizza lo stato degli agenti o dei connettori corrispondenti alla ricerca dell'utente. Ad esempio:

   ```
   Totale: 10 In esecuzione: 8 In sospeso: 1 Terminati: 1 Non risponde: 0
   ```

   Nota: l'aggiornamento della configurazione di un agente CA User Activity Reporting Module richiede al massimo cinque minuti per sincronizzare l'aggiornamento dello stato dell'agente con gli altri agenti presenti nella federazione.

7. (Facoltativo) Fare clic sulla visualizzazione dello stato per visualizzare i dettagli nel riquadro Stato in fondo al grafico

   Nota: è possibile fare clic sul pulsante Su richiesta di un agente o un connettore per aggiornare la visualizzazione dello stato.

8. (Facoltativo) Se si stanno visualizzando i connettori, selezionare qualsiasi connettore e fare clic su Ravvia, Avvia o Interrompi. Se si stanno visualizzando gli agenti, selezionare qualsiasi agente e fare clic su Riavvia.

Modalità di creazione di un gruppo di agenti

È possibile creare un gruppo di agenti per organizzare i propri agenti in base al luogo, al sistema operativo o a qualsiasi altra categoria adatta. Il procedimento di creazione di un gruppo di agenti utilizzando la procedura guidata Gruppo di agenti si basa sui passaggi seguenti:

1. Apertura della procedura guidata Gruppo di agenti.
2. Inserimento dei dettagli del gruppo.
3. Aggiunta degli agenti.

Ulteriori informazioni

Apertura della procedura guidata Gruppo di agenti (a pagina 669)
Aggiunta dei dettagli del gruppo di agenti (a pagina 670)

Apertura della procedura guidata Gruppo di agenti

Per creare un nuovo gruppo di agenti o modificarne uno esistente, aprire la procedura guidata Gruppo di agenti.

Per aprire la procedura guidata Gruppo di agenti

1. Fare clic sulla scheda Amministrazione, e quindi sulla sottoscheda Raccolta registri.

   Verrà visualizzato l'elenco cartella di Raccolta registri.

2. Fare clic sulla cartella Explorer agente.

   Nel riquadro dei dettagli vengono visualizzati i pulsanti di gestione agente.

3. Fare clic su Nuovo gruppo di agenti:

   Verrà visualizzata la procedura guidata Gruppo di agenti.

   Quando si utilizza la procedura guidata:

   - Fare clic su Salva per memorizzare il file senza chiudere la procedura guidata.
   - Fare clic su Salva e chiudi per salvare il file e chiudere la procedura guidata.
   - Fare clic su Reimposta per ripristinare la visualizzazione della procedura guidata alle ultime impostazioni salvate.

Aggiunta dei dettagli del gruppo di agenti

È possibile aggiungere dettagli identificativi al proprio gruppo di agenti.

Per aggiungere dettagli ad un gruppo di agenti

1. Aprire la procedura guidata Gruppo di agenti.
2. Inserire un nome per il gruppo e una descrizione facoltativa a scopo di riferimento.
3. Selezionare la Modalità di invio evento
4. (Facoltativo) Immettere i primi caratteri del server che si desidera aggiungere nel campo Modello nome.

   I server che corrispondenti alla ricerca vengono visualizzati nell'area Disponibili.
5. Selezionare i server che si desidera aggiungere utilizzando il controllo pilota e disporli nell'ordine di visualizzazione desiderato all'interno del gruppo agenti utilizzando tasti freccia GIÙ e freccia SU.
6. Procedere con il passaggio successivo, oppure fare clic su Salva e chiudi.

   Facendo clic su Salva e chiudi si creerà il gruppo. In caso contrario, verrà visualizzato il passaggio prescelto.

Aggiunta di agenti ad un gruppo di agenti

È possibile aggiungere agenti ad un gruppo per scopi amministrativi. Ad esempio, si possono creare dei gruppi in base alla regione geografica o al sistema operativo.

Nota: le proprietà di un gruppo di agenti vengono applicate a tutti gli agenti del gruppo.

Per aggiungere agenti ad un gruppo

1. Aprire la procedura guidata Gruppo di agenti e procedere con il passaggio Agenti.
2. (Facoltativo) Selezionare i criteri di ricerca agente. Se non si inserisce alcun termine di ricerca, verranno visualizzati tutti gli agenti. Per restringere la propria ricerca, è possibile selezionare uno o più criteri fra i seguenti:
   - Gruppo di agenti: restituisce solo gli agenti assegnati al gruppo selezionato.
   - Piattaforma: restituisce solo gli agenti in esecuzione sulla piattaforma selezionata.
   - Modello Nome agente: restituisce solo gli agenti che contengono il modello specificato.
3. Fare clic su Cerca.

   Nell'area Agenti disponibili verranno visualizzati gli agenti corrispondenti alla propria ricerca.
4. Selezionare gli agenti da aggiungere utilizzando il controllo pilota e, agendo sulle frecce in su e in giù, disporli nell'ordine in cui si desidera appaiano nella visualizzazione del gruppo di agenti.

   Nota: non è possibile spostare un agente in un Gruppo agenti se non dispne di un server CA User Activity Reporting Module configurato.
5. Fare clic su Salva, quindi su Chiudi.

   Nell'elenco verrà visualizzato il gruppo di agenti.

Nota: se si elimina un gruppo di agenti creato dall'utente, gli agenti contenuti in tale gruppo vengono trasferiti nel Gruppo agenti predefinito ed ereditano le proprietà del gruppo predefinito.

Modalità di configurazione della gestione agente

È possibile configurare i propri agenti, o gruppi di agenti, per fare rapporto ai diversi server di CA User Activity Reporting Module nel proprio ambiente federato. Così facendo sarà possibile configurare agenti o gruppi in modo da inviare informazioni di evento ai server CA User Activity Reporting Module designati.

Il procedimento di configurazione della gestione agenti tramite la procedura guidata di assegnazione dei server Log Manager prevede i seguenti passaggi:

1. Apertura della procedura guidata di assegnazione Server Log Manager.
2. Selezione dell'agente, o del gruppo di agenti, di destinazione da assegnare.
3. Selezione dei server CA User Activity Reporting Module per l'assegnazione di agenti o gruppi.

Ulteriori informazioni

Apertura della procedura guidata di assegnazione Server Log Manager (a pagina 673)
Selezione degli agenti di destinazione (a pagina 674)
Selezione dei server Log Manager (a pagina 675)

Apertura della procedura guidata di assegnazione Server Log Manager

Per configurare le assegnazioni dell'agente o del gruppo agenti, aprire la procedura guidata di assegnazione Server Log Manager.

Per aprire la procedura guidata di assegnazione Server Log Manager

1. Fare clic sulla scheda Amministrazione, e quindi sulla sottoscheda Raccolta registri.

   Verrà visualizzata la cartella Raccolta registri, che mostra i pulsanti di gestione agente posti nel riquadro dei dettagli.

2. Fare clic su Server Log Manager:

   Verrà visualizzata la procedura guidata di assegnazione Server Log Manager.

   Quando si utilizza la procedura guidata:

   - Fare clic su Salva per salvare la procedura guidata senza chiuderla.
   - Fare clic su Salva e chiudi per salvare l'assegnazione e chiudere la procedura guidata.
   - Fare clic su Reimposta per ripristinare la visualizzazione della procedura guidata alle ultime impostazioni salvate.

Ulteriori informazioni

Modalità di configurazione della gestione agente (a pagina 672)
Selezione degli agenti di destinazione (a pagina 674)
Selezione dei server Log Manager (a pagina 675)

Selezione degli agenti di destinazione

Per assegnare gli agenti ad un server per la ricezione e l'archiviazione degli eventi, si deve scegliere quale agente o gruppo assegnare ad uno specifico server CA User Activity Reporting Module.

Per selezionare gli agenti di destinazione

1. Aprire la procedura guidata di assegnazione Server Log Manager.
2. Scegliere se assegnare gli agenti singolarmente o in base al gruppo.
3. Se si sceglie Gruppi, utilizzare il controllo pilota per selezionare i gruppi da assegnare. È possibile utilizzare il campo di ricerca per individuare i gruppi digitando parte del loro nome. Durante la digitazione, i gruppi disponibili saranno filtrati.
4. Se si sceglie Agenti, utilizzare il controllo pilota per selezionare i singoli agenti da assegnare. Per individuare gli agenti, è possibile utilizzare gli elenchi a discesa Gruppo di agenti e Piattaforma, oltre al campo di ricerca.
5. Proseguire fino al passaggio Seleziona Log Manager.

Ulteriori informazioni

Modalità di configurazione della gestione agente (a pagina 672)
Apertura della procedura guidata di assegnazione Server Log Manager (a pagina 673)
Selezione dei server Log Manager (a pagina 675)

Selezione dei server Log Manager

Si deve scegliere a quale server di CA User Activity Reporting Module assegnare gli agenti o i gruppi di agenti.

Per selezionare i server Log Manager

1. Aprire la procedura guidata di assegnazione Server Log Manager e selezionare gli agenti di destinazione; quindi, procedere con il passaggio di selezione dei Log Manager.
2. Usare il controllo pilota per selezionare i server a cui si desidera assegnare gli agenti o i gruppi di agenti. Per eseguire delle ricerche nell'elenco disponibile, è possibile utilizzare il campo di inserimento Modello nome.
3. Fare clic su Salva e chiudi.

   L'agente o gli agenti raggruppati saranno assegnati ai server selezionati.

Ulteriori informazioni

Modalità di configurazione della gestione agente (a pagina 672)
Apertura della procedura guidata di assegnazione Server Log Manager (a pagina 673)
Selezione degli agenti di destinazione (a pagina 674)

Modalità di protezione degli agenti dalle conseguenze dei cambi di indirizzo IP dei server

Quando si installa un agente, si assegnerà ad esso un server CA User Activity Reporting Module principale che si dovrà contattare per primo dopo aver raccolto gli eventi. Quando si configura un agente, è possibile aggiungere altri server CA User Activity Reporting Module in un elenco ordinato. Quando un agente pronto ad inviare i registri raccolti al server primario non riesce a contattare quest'ultimo, l'agente contatta ogni server secondario nell'elenco finché non ne trova uno disponibile. La configurazione di un elenco ordinato di server secondari garantisce il recapito dei registri da un agente a un server. Un agente può inviare eventi solo a un CA User Activity Reporting Module per volta. In altre parole, la duplicazione degli eventi è impossibile.

Quando si assegnano nuovi indirizzi IP a uno o più server selezionati per gestire un agente, la capacità dell'agente di inoltrare gli eventi raccolti ad un server nell'elenco potrebbe risentirne. Adottando adeguate precauzioni, è possibile fare in modo che i server mantengano la massima disponibilità per gli agenti che li utilizzano, anche se subiscono la riassegnazione manuale o dinamica dell'indirizzo IP.

L'indirizzo IP di un CA User Activity Reporting Module installato può cambiare nei seguenti casi:

- Riassegnazione dinamica via DHCP

  Il server CA User Activity Reporting Module di un sistema single-server è configurato in modo da ricevere un indirizzo IP via DHCP. Dopo aver selezionato tale server per gestire gli agenti, DCHP assegnerà ad esso un nuovo indirizzo IP. Ciò può avvenire quando CA User Activity Reporting Module resta offline per un periodo tanto lungo da far scadere il lease dell'indirizzo IP. L'utente non riceverà alcuna notifica del cambio dinamico degli indirizzi IP.

- Riassegnazione manuale

  I server CA User Activity Reporting Module sono configurati con indirizzi IP statici. Poiché esiste un processo aziendale in cui gli indirizzi IP vengono riassegnati nell'ambito della distribuzione di una nuova sottorete, i nuovi indirizzi IP vengono assegnati ai server CA User Activity Reporting Module manualmente.

Nel caso in cui gli indirizzi IP dei server dovessero cambiare, eseguire gli interventi corretti per assicurare agli agenti il massimo della disponibilità dei server.

Ulteriori informazioni:

Garantire la disponibilità dei server con indirizzi IP dinamici (a pagina 677)
Garantire la disponibilità dei server durante la riassegnazione degli indirizzi IP statici (a pagina 677)

Garantire la disponibilità dei server con indirizzi IP dinamici

Se si seleziona DHCP nell'installare un CA User Activity Reporting Module single-server, quando si installa ogni agente, indicare il nome host (non l'indirizzo IP) di tale CA User Activity Reporting Module. In questo modo sarà possibile garantire che ogni riassegnazione DHCP dell'indirizzo IP del server CA User Activity Reporting Module non influenzerà gli agenti che lo utilizzano.

Se si specifica l'indirizzo IP del server CA User Activity Reporting Module durante l'installazione degli agenti e se tale indirizzo dinamico dovesse cambiare, sarà necessario reinstallare gli agenti in modo da ripristinare la disponibilità del server CA User Activity Reporting Module del singolo sistema. Per evitare questo potenziale problema, è consigliabile installare un server CA User Activity Reporting Module aggiuntivo ed aggiungerlo a tutti gli agenti come secondario. In questo modo si garantirà la disponibilità massima dei server.

Garantire la disponibilità dei server durante la riassegnazione degli indirizzi IP statici

Se si installano dei server CA User Activity Reporting Module con indirizzi IP statici, ed in seguito si decide di cambiarne la numerazione, utilizzare il seguente flusso di lavoro per offrire agli agenti la massima disponibilità dei server sui loro elenchi ordinati. Non è necessario riavviare l'agente dopo ogni passaggio poiché, per impostazione predefinita, esso aggiornerà la sua configurazione ogni 5 minuti.

Importante: se si configura un agente con un solo server CA User Activity Reporting Module all'interno di un sistema con server multipli, prima di assegnare i nuovi indirizzi IP, assicurarsi di aggiungere un secondo server all'elenco ordinato. In caso contrario, per ripristinare la disponibilità del server, potrebbe essere necessario reinstallare e riconfigurare l'agente dopo l'assegnazione dell'indirizzo IP al server.

Per consentire agli agenti di raggiungere un server CA User Activity Reporting Module presente nel loro elenco ordinato durante la riassegnazione dell'indirizzo IP statico ai server

1. Se si progetta di riassegnare gli indirizzi IP ad un server CA User Activity Reporting Module unico, installare un CA User Activity Reporting Module temporaneo che esegua un reindirizzamento a CA EEM sul CA User Activity Reporting Module originale.
2. Se uno o più server CA User Activity Reporting Module aggiuntivi non sono stati configurati per un qualsiasi agente di un sistema a più server, assegnare almeno un server aggiuntivo all'elenco ordinato.
   a. Selezionare Explorer agente e fare clic su Server Log Manager.

      Verrà visualizzata la la procedura guidata di assegnazione Server Log Manager e il passaggio Seleziona destinazioni sarà attivato.
   b. Selezionare gli agenti o i gruppi a seconda del modo in cui si eseguono tali assegnazioni.
   c. Selezionare i gruppi o gli agenti interessati come destinazione dall'elenco Disponibili, e spostarli nell'elenco Selezionati.
   d. Fare clic sul passaggio Seleziona server Log manager.
   e. Selezionare un CA Enterprise Log Manager dall'elenco Disponibili, e spostarlo nell'elenco Selezionati.
   f. Fare clic su Salva e chiudi.
3. Con la procedura guidata di assegnazione Server Log Manager, eliminare metà della lista ordinata dei server CA User Activity Reporting Module dalla configurazione dell'agente o del gruppo degli agenti.
4. Assegnare il nuovo indirizzo IP statico ai server eliminati dall'elenco selezionato.
5. Aggiungere nuovamente i server con i nuovi indirizzi IP.
6. Attendere che l'agente aggiorni le proprie informazioni di configurazione.

   Nota: è possibile riavviare manualmente l'agente in modo da aggiornare immediatamente le informazioni.
7. Eliminare l'altra metà dell'elenco ordinato.

   Nota: nel caso in cui si aggiunga un server temporaneo, lo si può conservare per scopi di failover, oppure disinstallarlo ed eliminarlo.
8. Riassegnare tali indirizzi IP.
9. Aggiungere nuovamente tali server in modo da ripristinare l'elenco ordinato originale.

Ulteriori informazioni:

Modalità di configurazione della gestione agente (a pagina 672)
Eliminazione di un host di servizio (a pagina 145)

Modalità di applicazione degli aggiornamenti di sottoscrizione

È possibile applicare gli aggiornamenti di sottoscrizione di CA ad agenti o connettori. Il processo di applicazione dei pacchetti di sottoscrizione utilizzando la procedura guidata Elenco aggiornamenti si basa sui seguenti passaggi:

1. Apertura della procedura guidata Elenco aggiornamenti.
2. Selezione di uno dei seguenti tipi di aggiornamento, ed indicazione dei criteri di ricerca per i pacchetti di aggiornamento disponibili:
   - Aggiornamenti agente
   - Aggiornamenti di integrazione per i connettori.

   Nota: se sono disponibili aggiornamenti per agenti e connettori, per completare l'aggiornamento occorre applicare prima gli aggiornamenti agli agenti.
3. Selezione agenti o connettori da aggiornare all'ultima versione.

Ulteriori informazioni

Apertura della procedura guidata Elenco aggiornamenti (a pagina 680)
Selezione degli agenti o dei connettori da aggiornare (a pagina 681)
Aggiornamento delle versioni di integrazione dell'agente o del connettore (a pagina 682)

Apertura della procedura guidata Elenco aggiornamenti

Per aggiornare gli agenti o i connettori all'ultima versione, aprire la procedura guidata Elenco aggiornamenti.

Per aprire la procedura guidata Elenco aggiornamenti

1. Fare clic sulla scheda Amministrazione e quindi sulla sottoscheda Raccolta registri.

   Apparirà l'elenco della cartella Raccolta registri.

2. Fare clic sulla cartella Explorer agente.

   Nel riquadro dei dettagli verranno visualizzati i pulsanti relativi alla gestione agenti.

3. Fare clic su Sottoscrizione:

   Verrà visualizzata la procedura guidata Elenco aggiornamenti.

   Quando si utilizza la procedura guidata:

   - Fare clic su Salva per salvare il file senza chiudere la procedura guidata.
   - Fare clic su Salva e chiudi per salvare i propri progressi e chiudere la procedura guidata.
   - Fare clic su Reimposta per riportare la visualizzazione della procedura guidata alle ultime impostazioni salvate.

Selezione degli agenti o dei connettori da aggiornare

È possibile controllare gli aggiornamenti disponibili specificando i criteri di ricerca per gli agenti o i connettori candidati.

Per selezionare gli agenti o i connettori da aggiornare

1. Aprire la procedura guidata Elenco aggiornamenti.

   Verrà visualizzata la procedura guidata Elenco selezione aggiornamenti.

2. Selezionare Aggiornamenti agente o Aggiornamenti connettore.

   Nota: se sono disponibili aggiornamenti per agenti e connettori, per completare l'aggiornamento occorre applicare prima gli aggiornamenti agli agenti.

3. Completare i criteri di ricerca degli aggiornamenti per l'agente o per il connettore:

   a. Selezionare un Gruppo di agenti dall'elenco a discesa.

   b. Selezionare la piattaforma dall’elenco a discesa.

   c. Digitare il modello del nome dell'agente utilizzando i caratteri jolly.

   d. (Solo per aggiornamenti di integrazione del connettore) Selezionare l'integrazione dall'elenco a discesa.

4. Fare clic su Cerca.

   Nel successivo passaggio della procedura guidata, ovvero Selezione versione, verranno visualizzati i pacchetti di aggiornamento che corrispondono alle proprie qualifiche di ricerca. Per visualizzarli ed applicarli si deve proseguire con il passaggio Selezione versione.

Ulteriori informazioni:

Apertura della procedura guidata Elenco aggiornamenti (a pagina 680)
Aggiornamento delle versioni di integrazione dell'agente o del connettore (a pagina 682)

Aggiornamento delle versioni di integrazione dell'agente o del connettore

È possibile confrontare la versione di ogni agente o connettore elencato con quelle dell'aggiornamento scaricato, in modo da stabilire se sia necessario aggiornare e per scegliere se sostituire la versione attuale con una diversa.

Per aggiornare gli agenti o i connettori

1. Aprire la procedura guidata Elenco aggiornamenti e selezionare gli agenti o i connettori che si desidera prendere in considerazione per l'aggiornamento.
2. Proseguire fino al passaggio Selezione versione.

   Viene visualizzato l'elenco degli agenti o dei connettori corrispondenti ai propri criteri di ricerca.

   - Ogni agente viene visualizzato con la sua versione attuale e con un elenco a discesa contenente le versioni di aggiornamento disponibili.
   - Ogni connettore viene visualizzato con la sua versione di integrazione attuale e con un elenco a discesa contenente le versioni di aggiornamento disponibili.
3. (Facoltativo) Selezionare Versione sistema operativo bypass per visualizzare tutti gli aggiornamenti disponibili per il proprio sistema operativo, indipendentemente dalla versione.
4. Selezionare gli agenti o i connettori a cui si desidera applicare gli aggiornamenti e fare clic su Salva e chiudi.

   L'agente installerà gli aggiornamenti, sostituendo la versione attuale con l'aggiornamento selezionato dell'agente o dell'integrazione.

Nota: se si controllano tali dettagli dopo l'applicazione degli aggiornamenti selezionati si potrà verificare se tutti gli agenti o connettori abbiano applicato la versione più recente.

Creazione di un file di diagnosi agente per il Supporto

È possibile esaminare i file di log e i file di configurazione dell'agente CA User Activity Reporting Module selezionato. L'utilità AgentDiagnostics riunisce le informazioni di sistema e i file di log in un file compresso .tar per l'invio al Supporto di CA Technologies. È possibile trasmettere questo file tramite FTP o altro metodo di trasferimento dei file.

Nota: è possibile che il file contenga informazioni riservate, quali indirizzi IP, configurazioni di sistema, log hardware e log dei processi. Utilizzare un metodo protetto per memorizzare e trasferire questo file.

Per creare un file di diagnosi agente

1. Accedere alla directory dei file binari agente di CA User Activity Reporting Module.

   Percorso predefinito per Windows: C:\Program Files\CA\elmagent\bin

   Percorso predefinito per UNIX/Linux: /opt/CA/ELMagent/bin

2. Eseguire *una* delle operazioni indicate di seguito:

   a. Se l'agente viene eseguito su un sistema Windows, eseguire il file AgentDiagnostics.bat.

   b. Se l'agente viene eseguito su un sistema UNIX/Linux, eseguire il file AgentDiagnostics.sh file.

   Viene creato un file di diagnosi agente con formato *agenthostname_DDMMYYYY_HHMM*.tar.gz

Capitolo 22: Certificati personalizzati

Questa sezione contiene i seguenti argomenti:

Implementazione di certificati personalizzati (a pagina 685)
Aggiunta del Certificato radice attendibile al server di gestione CA User Activity Reporting Module (a pagina 686)
Aggiunta del Certificato radice attendibile a tutti gli altri server CA User Activity Reporting Module (a pagina 688)
Aggiunta del nome comune di certificato ad un criterio di accesso (a pagina 689)
Distribuzione dei nuovi certificati (a pagina 690)

Implementazione di certificati personalizzati

Il processo di installazione genera due certificati e li inserisce nella directory /opt/CA/SharedComponents/iTechnology del server CA User Activity Reporting Module. È possibile utilizzare il certificato installato senza apportare ulteriori modifiche. I certificati sono denominati nella seguente maniera, in cui *ApplicationName* corrisponde a CAELM per il prodotto CA User Activity Reporting Module.

- *ApplicationName*Cert.cer

  Tutti i servizi di CA User Activity Reporting Module utilizzano questo certificato per comunicare con il server di gestione. La voce di questo certificato esiste già nel file CALM.cnf.

- *ApplicationName*_AgentCert.cer

  Tutti gli agenti utilizzano questo certificato per comunicare con i server CA User Activity Reporting Module.

  Importante: La sostituzione del certificato CAELM_AgentCert.cer con un certificato personalizzato in un ambiente con agenti attivi richiede la reinstallazione degli agenti stessi.

Per utilizzare i certificati personalizzati, è necessario ottenere un Certificato radice attendibile da un'autorità di certificazione principale (CA). Un'autorità di certificazione può emettere più certificati sottoforma di struttura ad albero. Tutti i certificati conformi al certificato radice attendibile ereditano l'attendibilità del certificato radice. Il processo presuppone che, se entrambi i certificati vengono sostituiti, i certificati di servizio personalizzato e di agente presentano la stessa radice attendibile.

Sono supportati solo i certificati personalizzati con estensioni .cer. Dopo avere ottenuto un certificato radice attendibile, attenersi alla sequenza di azioni riportata di seguito per l'implementazione dei certificati personalizzati:

1. Aggiungere il Certificato radice attendibile a iAuthority.conf del server di gestione CA User Activity Reporting Module o del server autonomo CA EEM.
2. Se si sostituisce CAELM_AgentCert.cer, aggiungere il Certificato radice attendibile a iControl.conf del server di gestione CA User Activity Reporting Module, quindi ripetere l'operazione per ogni altro server CA User Activity Reporting Module.
3. Se si sostituisce CAELMCert.cer, aggiungere questo nome comune del certificato personalizzato al criterio di scoping AdministerObjects del server di gestione CA User Activity Reporting Module o del server autonomo CA EEM.
4. Aggiungere i certificati personalizzati alla cartella iTechnology di ogni server CA User Activity Reporting Module, quindi aggiungere il nome e la password per ogni certificato in file di configurazione separati.

Aggiunta del Certificato radice attendibile al server di gestione CA User Activity Reporting Module

In primo luogo, è necessario ottenere dall'Autorità di certificazione (CA) un Certificato radice attendibile in formato PEM. Quindi aggiungere il certificato all'interfaccia Web iTechnology SPIN del server di gestione o del server autonomo CA EEM.

Per aggiungere il Certificato radice attendibile al server CA User Activity Reporting Module di gestione

1. Accedere all'interfaccia Web iTechnology SPIN di CA del server di gestione CA User Activity Reporting Module o del server autonomo CA EEM.

   ```
   https://<management_ELM_hostname>:5250/spin
   ```

   ```
   https://<EEM_hostname>5250/spin
   ```

   Verrà visualizzata la pagina di CA iTechnology SPIN.
2. Dall'elenco a discesa selezionare amministratore iTech e fare clic su Vai a.

   Verrà visualizzata la pagina di amministrazione iTechnology con un collegamento di accesso.
3. Fare clic su Accedi.

   Verrà visualizzata la finestra di accesso CA iTechnology.

4. Immettere le credenziali di EiamAdmin, selezionare iAuthority, quindi fare clic su Accedi.
5. Selezionare la scheda iAuthority ed aggiungere la radice attendibile a iAuthority.conf attenendosi alle procedure descritte di seguito:
   a. Inserire un'etichetta per il certificato. Non immettere il nome stesso dell'utente come etichetta.
   b. Sfogliare e selezionare il file .cer.
   c. Fare clic su Aggiungi radice attendibile.

   Il messaggio di conferma indica che la radice attendibile è stata aggiunta a iAuthority.conf. Si tratta di un file presente soltanto nel server di gestione o nel server autonomo CA EEM.
6. Se si utilizza un server autonomo CA EEM, passare all'ultimo passaggio.
7. Se si desidera sostituire il certificato CAELM_AgentCert.cer con un certificato personalizzato, aggiungere la radice attendibile ad iControl.conf attenendosi alla procedura riportata di seguito:
   a. Selezionare la scheda di configurazione.
   b. Immettere la stessa etichetta per il certificato specificato nel passaggio precedente.
   c. Sfogliare e seleziona la stessa radice PEM (.cer) selezionata nel passaggio precedente.
   d. Fare clic su Aggiungi radice attendibile.

   Il messaggio di conferma indica che la radice attendibile del certificato personalizzato è stato aggiunto al file iControl.conf viene della directory iTechnology del server di gestione CA User Activity Reporting Module.
8. Fare clic su Disconnetti, quindi chiudere iTechnology SPIN.

Aggiunta del Certificato radice attendibile a tutti gli altri server CA User Activity Reporting Module

Se si desidera sostituire il certificato CAELM_AgentCert.cer con un certificato personalizzato, è necessario aggiungere il Certificato radice attendibile all'interfaccia Web iTechnology SPIN di ogni server CA User Activity Reporting Module aggiuntivo. La procedura consente di aggiungere il Certificato radice attendibile a CA iControl. Si tratta di una procedura non necessaria se si desidera sostituire soltanto il certificato CAELMCert.cer.

Per aggiungere il Certificato radice attendibile a CA iControl di ogni server non di gestione CA User Activity Reporting Module:

1. Accedere all'interfaccia utente SPIN del sistema iGateway in cui è in esecuzione il server non di gestione. Utilizzare il seguente URL:

   ```
   https://<ELM_hostname>:5250/spin/
   ```

   Verrà visualizzata la pagina di CA iTechnology SPIN.

2. Dall'elenco a discesa selezionare amministratore iTech e fare clic su Vai a.

   Verrà visualizzata la pagina di amministrazione iTechnology con un collegamento di accesso.

3. Fare clic su Accedi.

   Verrà visualizzata la finestra di accesso CA iTechnology.

4. Immettere le credenziali di EiamAdmin, selezionare iAuthority, quindi fare clic su Accedi.

5. Selezionare la scheda di configurazione ed aggiungere la radice attendibile secondo la modalità riportata di seguito:

   a. Immettere la stessa etichetta per il certificato specificato nel passaggio precedente.

   b. Sfogliare e selezionare il file .cer.

   c. Fare clic su Aggiungi radice attendibile.

   La radice attendibile del certificato personalizzato è stata aggiunta al file iControl.conf della directory iTechnology. Viene visualizzato un messaggio di conferma.

6. Fare clic su Disconnetti, quindi chiudere iTechnology SPIN.

Aggiunta del nome comune di certificato ad un criterio di accesso

Tutti i servizi di CA User Activity Reporting Module utilizzano il certificato CAELMCert.cer per comunicare con il server di gestione CA User Activity Reporting Module. Se si sostituisce CAELMCert.cer con un certificato personalizzato, è necessario aggiungere questo nome comune del certificato personalizzato (CN) al criterio AdministerObjects del server di gestione CA User Activity Reporting Module o del server autonomo CA EEM.

Nota: non è necessario eliminare l'identità [User] CERT_CAELM, ossia il nome comune del certificato predefinito, dal criterio.

Per aggiungere il nome comune del certificato personalizzato al criterio AdministerObjects

1. Accedere al server di gestione CA User Activity Reporting Module o al server autonomo CA EEM inserendo l'URL appropriato.

   ```
   https://<management_server_hostname>:5250/spin/calm
   ```

   ```
   https://<EEM_server_hostname>:5250/spin/eiam
   ```

2. Accedere al server di gestione CA User Activity Reporting Module come utente con privilegi di amministrazione. Se si effettua l'accesso ad un server autonomo CA EEM, accedere come utente EiamAdmin.
3. Fare clic sulla scheda Amministrazione, la sottoscheda Gestione utenti e accessi, quindi sul collegamento Criteri di accesso e il collegamento Criterio di accesso nel riquadro a sinistra. Se si è connessi a un server autonomo CA EEM, fare clic sulla scheda di gestione dei criteri di accesso.
4. Fare clic sul collegamento Criteri di scoping.

   Nel pannello principale verrà visualizzata la tabella dei criteri di scoping.

5. Scorrere al criterio AdministerObjects e selezionare il collegamento AdministerObjects.

   Si aprirà il criterio AdministerObjects in modalità di modifica.

6. Aggiungere il nome comune (CN) del certificato personalizzato attenendosi alla procedura riportata di seguito:
   a. Inserire il nome comune del certificato personalizzato nel campo Identità.
   b. Fare clic sulla freccia per spostare la propria voce.

      [User}<*custom certificate cn*> verrà visualizzato nell'elenco Identità selezionate.
7. Fare clic su Salva.

   Il criterio AdministerObjects sarà salvato, con l'aggiunta del nome comune del proprio certificato personalizzato, come identità con accesso in lettura e scrittura alle risorse elencate in tale criterio.
8. Fare clic su Chiudi per uscire dall'interfaccia utente di CA User Activity Reporting Module.

Distribuzione dei nuovi certificati

CA User Activity Reporting Module utilizza due certificati. È possibile sostituire uno o più certificati predefiniti con certificati personalizzati. Per distribuire i nuovi certificati, accedere all'applicazione software, arrestare iGateway, aggiungere i nuovi certificati, modificare i file di configurazione corrispondenti a riavviare iGateway.

Prima di distribuire i nuovi certificati, verificare che:

- Il Certificato radice attendibile sia stato aggiunto a iTechnology iAuthority del server di gestione o del server autonomo CA EEM utilizzato dai server CA User Activity Reporting Module.
- Se CAELM_AgentCert.cer viene sostituito con un certificato personalizzato, il Certificato radice attendibile viene aggiunto ad iTechnology iControl di ogni server CA User Activity Reporting Module.
- Il nome comune del certificato personalizzato sia stato aggiunto al criterio di accesso AdministerObjects. Si tratta del certificato personalizzato che sostituisce CAELMCert.cer

Per distribuire i nuovi certificati

1. Accedere all'host su cui è installato il server CA User Activity Reporting Module.
2. Utilizzare le proprie credenziali di **caelmadmin** per accedere al server CA User Activity Reporting Module.
3. Dal prompt dei comandi, commutare gli utenti su root, ovvero:

   ```
   su - root
   ```

4. Modificare la directory in /opt/CA/SharedComponents/iTechnology usando il seguente collegamento:

   ```
   cd $IGW_LOC
   ```

5. Arrestare iGateway.

   ```
   ./S99igateway stop
   ```

6. Per sostituire caelmcert.cer:
   a. Copiare il certificato personalizzato *ApplicationName*Cert.cer ed il file di chiave *ApplicationName*Cert.key nella directory iTechnology.
   b. Aprire il file CALM.cnf. Sostituire il nome del certificato con il nuovo nome.
   c. Sostituire il nome del file di chiave esistente con il nuovo nome del file.
7. Per sostituire CAELM_AgentCert.cer:
   a. Copiare il certificato personalizzato *ApplicationName*_AgentCert.cer ed il file di chiave *ApplicationName*_AgentCert.key nella directory iTechnology.
   b. Aprire il file AgentManager.conf. Sostituire il nome del certificato con il nuovo nome.
   c. Sostituire il nome del file di chiave esistente con il nuovo nome del file.
8. Avviare iGateway.

   ```
   ./S99igateway start
   ```

   Se CAELM_AgentCert.cer viene sostituito, tutti gli agenti installati dopo la distribuzione utilizzeranno automaticamente il certificato personalizzato.

Appendice A: Funzionalità di accessibilità

CA si impegna ad assicurare a tutti i clienti, indipendentemente dalle capacità, la possibilità di utilizzare appieno i propri prodotti e la documentazione di supporto allo scopo di completare operazioni aziendali di importanza vitale. Questa sezione illustra le funzionalità di accessibilità contenute in CA User Activity Reporting Module.

Modalità di accessibilità

È possibile impostare CA User Activity Reporting Module in modo da utilizzare una modalità di accessibilità, utile per visualizzare tutti i pannelli grafici nelle query e nei rapporti sotto forma di tabelle. Per accedere alla modalità di accessibilità, nella schermata di accesso selezionare la casella Attiva accessibilità.

Controlli di accessibilità

È possibile utilizzare i controlli di tastiera per navigare in CA User Activity Reporting Module, come illustrato nella seguente tabella:

Attività	Controlli di tastiera
Passare da un'applicazione aperta all'altra	CTRL-TAB
Selezionare un file in una finestra aperta	CTRL-TAB
?	F1
Clic su un pulsante	Spazio o Invio
Selezione di casella di controllo	Spazio o Invio
Menu aperto, casella combinata	CTRL + Freccia in giù
Elenco navigazione	CTRL + Freccia in giù per attivare Freccia in su o in giù per navigare Spazio o invio per selezionare un elemento dell'elenco

Attività	Controlli di tastiera
Pulsante di opzione Gruppo	CTRL + Freccia in giù per attivare Freccia in su o in giù per navigare Spazio o invio per selezionare un elemento dell'elenco
Chiudere la finestra attiva	ALT + F4
Doppio clic	CTRL + D

Impostazioni CA User Activity Reporting Module della lingua di visualizzazione

L'interfaccia CA User Activity Reporting Module può essere visualizzata, oltre che in inglese, nelle lingue seguenti:

- Francese
- Italiano
- Tedesco
- Spagnolo
- Giapponese

Modificare le impostazioni della lingua dalla finestra del browser. Ad esempio, se si utilizza Microsoft Internet Explorer, aprire la finestra di dialogo Opzioni Internet e aggiungere o selezionare la lingua primaria desiderata.

Se si seleziona una delle cinque lingue supportate, al successivo avvio l'interfaccia CA User Activity Reporting Module verrà visualizzata nella lingua appropriata. Le etichette e le schede dell'interfaccia sono state tradotte, ma alcuni elementi, come per esempio titoli di tag o stringhe di dati dei risultati dei rapporti sono stati mantenuti in inglese.

Nota: se si visualizza CA User Activity Reporting Module mentre si apportano le modifiche, aggiornare la finestra del browser per visualizzare la nuova lingua. Se durante questa operazione l'utente è collegato, verrà reindirizzato alla schermata di accesso nella nuova lingua.

Localizzazione manuale di CA User Activity Reporting Module

È possibile localizzare manualmente CA User Activity Reporting Module creando file di lingua personali. Ciò consente di visualizzare l'interfaccia di CA User Activity Reporting Module in lingue diverse da quelle già supportate. È possibile eseguire tale operazione copiando i file esistenti per poi utilizzarli come modelli.

Per localizzare manualmente CA User Activity Reporting Module

1. Accedere al proprio host del server CA User Activity Reporting Module, passare alla directory opt/CA/LogManager/local e scegliere i file da utilizzare come modelli. Sono presenti due file per ogni lingua:

   - content.properties - contiene il testo che descrive diversi contenuti, come ad esempio i nomi dei rapporti e delle query e le descrizioni.
   - ui.properties - contiene le stringhe di testo per i titoli delle funzioni dell'interfaccia, come ad esempio le intestazioni e le etichette di scheda.

   Ogni file è preceduto da un prefisso standard di lingua. Ad esempio, il file di contenuto per la lingua tedesca si chiama de_content.properties. Il file dell'interfaccia per la lingua inglese si chiama en_ui.properties.

2. Fare una copia di ogni tipo di file e rinominarlo utilizzando il prefisso standard. Ad esempio, per creare un file di localizzazione per la lingua portoghese copiare i file e rinominarli in pt_content.properties e pt__ui.properties.

   Nota: i prefissi standard della lingua si trovano nell'elenco delle lingue supportato dal browser dell'utente.

3. Aprire i file e tradurre le stringhe dalla lingua originale a quella desiderata. Ad esempio, dopo aver copiato i file per la lingua inglese è possibile sostituire ogni stringa di testo in inglese con la lingua desiderata.
4. Salvare i file tradotti manualmente nella posizione indicata nel passaggio 1 su ogni server CA User Activity Reporting Module in cui occorre utilizzarli.
5. Impostare il proprio browser nella lingua di destinazione e accedere a CA User Activity Reporting Module.

Ulteriori informazioni:

Impostazioni CA User Activity Reporting Module della lingua di visualizzazione (a pagina 694)

Appendice B: Accesso agli eventi raccolti con ODBC e JDBC

Questa sezione contiene i seguenti argomenti:

Informazioni sull'accesso ODBC/JDBC in CA User Activity Reporting Module (a pagina 697)
Creazione di query ODBC e JDBC da utilizzare con CA User Activity Reporting Module (a pagina 698)
Elaborazione delle query (a pagina 700)
Esempio: utilizzare un filtro di accesso per limitare i risultati ODBC (a pagina 702)
Esempio: preparazione all'utilizzo dei client ODBC e JDBC con Crystal Reports (a pagina 704)
Utilizzare Crystal Reports per accedere all'Archivio di registro eventi con ODBC (a pagina 711)
Accesso a Eventi da Crystal Reports con JDBC (a pagina 713)
Eliminare il client ODBC sui sistemi Windows (a pagina 715)
Rimozione del client JDBC (a pagina 715)

Informazioni sull'accesso ODBC/JDBC in CA User Activity Reporting Module

CA User Activity Reporting Module fornisce l'accesso ODBC e JDBC di sola lettura al deposito eventi di log per consentire l'esecuzione delle seguenti operazioni:

- Configurare rapporti personalizzati con un'utilità per la creazione di rapporti esterna, come Crystal Reports di BusinessObjects
- Recuperare informazioni sui log selezionati, tramite l'utilizzo di applicazioni esterne

Tali funzionalità consentono di creare e formattare rapporti personalizzati tramite le informazioni recuperate dal server CA User Activity Reporting Module. Inoltre, è possibile recuperare i dati da utilizzare con i motori di correlazione esistenti, i pacchetti di rilevamento malware e altre funzioni.

Una volta installato il client fornito da CA sul sistema da utilizzare per accedere al deposito eventi di log, configurare una connessione all'origine dati e iniziare il recupero dei dati. Il servizio di sottoscrizione installa i componenti lato server.

Creazione di query ODBC e JDBC da utilizzare con CA User Activity Reporting Module

Il supporto per ODBC e JDBC in CA User Activity Reporting Module è limitato alle query di sola lettura che utilizzano le istruzioni SELECT nelle seguenti tabelle:

- VIEW_EVENT - Contiene eventi del database eventi
- VIEW_INCIDENT - Contiene incidenti del database incidenti
- VIEW_INCIDENTEVENT_BYID - Contiene eventi del componente incidente del database eventi incidente

Creare istruzioni SELECT personalizzate utilizzando le regole ed il formato ANSI SQL. I componenti lato server contengono un motore di analisi SQL. L'analizzatore implementa gran parte di SQL di base come definito nella specifica X3.135-1992 "Database Language SQL". L'analizzatore supporta inoltre le funzioni SQL di ANSI SQL99 e database commerciali come Microsoft SQL Server e Oracle. L'analizzatore è conforme alle specifiche minime di grammatica ODBC.

La grammatica evento comune funge da schema di questa tabella. Consultare la *Guida di riferimento CEG* per informazioni sullo schema.

Limitazioni del supporto SQL

CA User Activity Reporting Module non supporta le chiamate stored procedure, i comandi del linguaggio di controllo dei dati (DCL) e del linguaggio di definizione dei dati (DDL).

CA User Activity Reporting Module non supporta le seguenti operazioni e parole chiave del linguaggio di modifica dei dati (DML):

- UNION
- JOIN
- SELECT nidificato
- INSERT
- AGGIORNA
- DELETE
- Operatori di controllo della transazione, come COMMIT, ROLLBACK e così via.

Funzioni SQL supportate

Le funzioni SQL seguenti sono supportate per la creazione di istruzioni SELECT:

- ABS(*numeric_exp*)
- ROUND(*numeric_exp, integer_exp*)
- LCASE(*string_exp*)
- LOWER(*string_exp*)
- LENGTH(*string_exp*)
- LTRIM(*string_exp*)
- RTRIM(*string_exp*)
- SUBSTRING(*string_exp, start,length*)
- UCASE(*string_exp*)
- UPPER(*string_exp*)
- IFNULL (*expr, default_val*)
- ISNULL (*expr, default_val*)
- NVL (*expr, default_val*)
- CONVERT (*value_exp, data_type*)
- CURDATE()
- CURTIME()
- CURTIMESTAMP()
- DATEADD(*datepart, number, date*)
- TIMESTAMPADD(*datepart, number, date*)
- DATEDIFF(*datepart, startdate, enddate*) Per la funzione datepart, sono consentiti i valori anno, giorno e secondo.
- TIMESTAMPDIFF(*datepart, startdate, enddate*) Per la funzione datepart, sono consentiti i valori anno, giorno e secondo.
- DAYOFMONTH(*date_exp*)
- DAYOFWEEK(*date_exp*)
- DAYOFYEAR(*date_exp*)
- HOUR(*time_exp*)

- MINUTE(*time_exp*)
- MONTH(*date_exp*)
- NOW( )
- SECOND(*time_exp*)
- WEEK(*date_exp*)
- YEAR(*date_exp*)
- AVG([ALL | DISTINCT]*expression*)
- SUM([ALL | DISTINCT]*expression*)
- COUNT({[ALL | DISTINCT]*expression*] | *})
- MAX([ALL | DISTINCT]*expression*)
- MIN([ALL | DISTINCT]*expression*)

Elaborazione delle query

CA User Activity Reporting Module elabora una query avviata dal client ODBC o JDBC nel modo seguente:

1. Un'applicazione client invia al server CA User Activity Reporting Module un'istruzione SELECT tramite una connessione ODBC.
2. L'istruzione SELECT verrà convalidata da CA User Activity Reporting Module. Se la convalida viene completata correttamente, il server CA User Activity Reporting Module crea una struttura di dati che rappresenta la query.

   Eventuali errori riscontrati vengono restituiti direttamente al driver client.
3. Il server CA User Activity Reporting Module converte gli elementi SQL in una query che potrà utilizzare. Se la conversione viene eseguita con successo, il server CA User Activity Reporting Module eseguirà la query.

   Eventuali errori riscontrati vengono restituiti al driver client.
4. CA User Activity Reporting Module gestisce le informazioni sullo stato di ciascuna query, inclusa la data di scadenza, consentendone l'annullamento nel caso in cui si chiudesse la sessione o scadesse la query.
5. Il server CA User Activity Reporting Module traduce i risultati della query, li invia nuovamente al driver client ODBC consentendo all'applicazione client di ricevere i dati.

Alias delle colonne di risultati

Nell'ambito della gestione dello stato della query, CA User Activity Reporting Module fornisce supporto per i nomi delle colonne di risultati con alias. Di conseguenza, tramite le etichette e le intestazioni, è possibile visualizzare i campi della grammatica evento comune nei rapporti personalizzati.

I nomi alias vengono mantenuti e utilizzati per eseguire correttamente il mapping dei dati quando il server CA User Activity Reporting Module trasferisce i risultati al driver client.

Limiti risultato

Per gestire lo spazio su disco, CA User Activity Reporting Module limita il numero delle righe di risultati. CA User Activity Reporting Module utilizza un sottoinsieme della parole chiave TOP di Transact-SQL con un solo valore fisso. Non è supportata la variante percentuale della parola chiave.

Il valore TOP predefinito in CA User Activity Reporting Module è 5000 righe e il valore massimo è 50.000.

Codici di errore specifici di CA User Activity Reporting Module

Di seguito sono riportati i codici di errore ODBC e JDBC che possono verificarsi mentre si effettua l'accesso all'archivio di registro eventi di CA User Activity Reporting Module. Ciascun messaggio di errore fornisce i dettagli specifici dell'errore in questione.

- 88: non supportato

  Il messaggio di errore correlato fornisce informazioni sulla funzionalità non supportata.

- 300: errore generico

  Il messaggio di errore correlato fornisce tutte le informazioni.

- 301: errore di conversione dei parametri dei caratteri multibyte
- 302: errore di autenticazione
- 304: espressione non valida (colonna) nelle clausole Ordina per e Raggruppa per

Di seguito sono riportati gli errori di esecuzione dell'istruzione SQL:

- 305: errore di avvio della query
- 306: errore nel rilevamento dello stato della query
- 307: errore nell'analisi del codice XML dei risultati della query
- 308: errore di esecuzione della query
- 309: query eseguita con errori
- 310: errore nel recupero dei risultati della query
- 311: timeout query

Esempio: utilizzare un filtro di accesso per limitare i risultati ODBC

È possibile creare un filtro di accesso per limitare i dati restituiti ad una richiesta di accesso ODBC. Quando i membri del gruppo applicazioni nominato accedono ai dati di evento CA User Activity Reporting Module utilizzando il client ODBC, vedranno solo le informazioni consentite dal filtro.

Questo esempio presume che l'utente disponga di un gruppo applicazioni denominato UNIX_Analysts e che voglia fare in modo che tutti i membri di quel gruppo visualizzino solo gli eventi UNIX dall'archivio di registro eventi. Il filtro creato in questo esempio limita le visualizzazioni dei dati dell'evento dall'interfaccia utente di CA User Activity Reporting Module e le richieste esterne tramite ODBC.

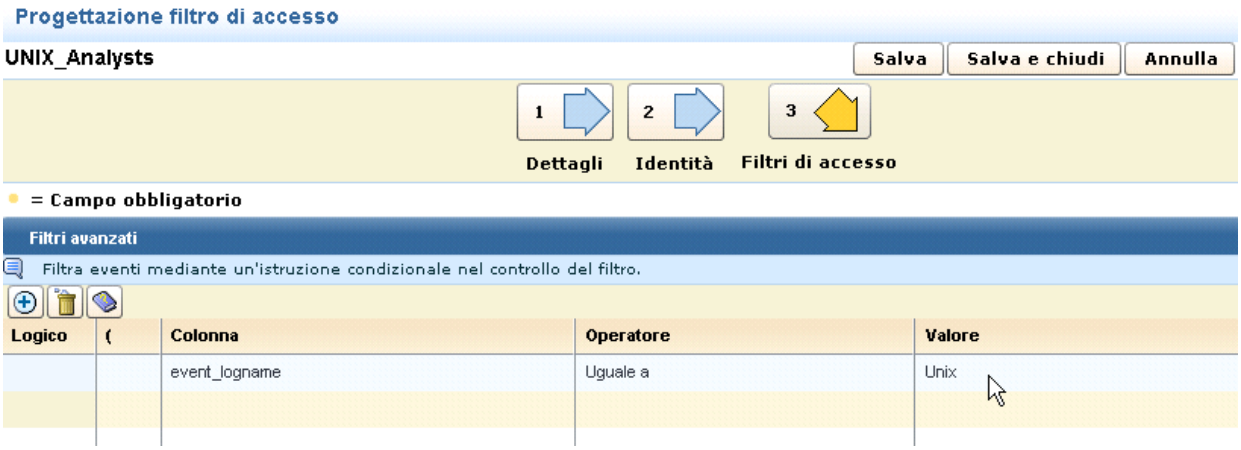
Ulteriori informazioni sui filtri di accesso sono disponibili nella Guida in linea.

Per creare un filtro di accesso

1. Accedere a CA User Activity Reporting Module come utente amministratore.
2. Fare clic sulla scheda Amministrazione e quindi sulla sottoscheda Gestione utenti e accessi.
3. Fare clic su Nuovo filtro di accesso . Verrà avviata la procedura guidata Progettazione filtro di accesso.

4. Immettere UNIX Analysts nel campo Nome e la frase Filtro di accesso a Unix Analysts in Descrizione e quindi fare clic sul passaggio 2 Identità, nella parte superiore della finestra di dialogo.
5. Cambiare il Tipo al Gruppo applicazioni e digitare UNIX nel campo Nome. Quindi, fare clic su Cerca identità.

   In un controllo pilota verrà visualizzato un elenco delle identità corrispondenti ai criteri di ricerca, in modo tale da consentire la selezione delle identità desiderate.
6. Selezionare il gruppo applicazione UNIX_Analysts dall'elenco Identità disponibili e fare clic sulla freccia destra del controllo pilota per spostare la selezione nell'elenco Identità selezionate.
7. Fare clic sul passaggio 3 Filtri di accesso, nella parte superiore della finestra di dialogo.
8. Fare clic su Nuovo filtro evento per aggiungere una riga e quindi fare clic nell'area del campo interessato in Colonna.
9. Selezionare event_logname dall'elenco a discesa e quindi fare clic nell'area del campo in Valore.
10. Selezionare UNIX dall'elenco a discesa. La finestra di dialogo visualizzata sarà simile a quella della figura seguente:



11. Fare clic su Salva e chiudi.

Esempio: preparazione all'utilizzo dei client ODBC e JDBC con Crystal Reports

La preparazione all'accesso del client ODBC o JDBC a eventi CA User Activity Reporting Module tramite BusinessObjects Crystal Reports si articola nei seguenti passaggi:

1. Creare un utente CA User Activity Reporting Module che consente l'accesso al database.
2. Verificare che il Servizio ODBC utilizzi la crittografia SSLe la porta 17002.
3. Installare il client ODBC oppure copiare i file di JDBC sul server in cui si trova Crystal Reports.

   Per informazioni relative a queste installazioni, consultare la *Guida all'implementazione*.
4. Configurare i componenti del sistema operativo:
   a. Creare ed eseguire un test sull'origine dati ODBC nel Pannello di controllo di Windows.
   b. Modificare il file di configurazione di Crystal Reports per utilizzare il client JDBC.
5. Creare eventi di raccolta tramite CA User Activity Reporting Module.

   Se l'archivio di registro eventi contiene già eventi del tipo interrogato dalla query, è possibile ignorare questo passaggio.

Nota: questo processo e gli esempi correlati presuppongono che l'utente abbia acquisito familiarità con la creazione di istruzioni SQL di base e l'utilizzo di Crystal Reports. Ulteriori informazioni sull'utilizzo di Crystal Reports sono disponibili nella guida in linea BusinessObjects.

Creazione di un utente CA User Activity Reporting Module per l'accesso ODBC o JDBC

Utilizzare questa procedura per creare un account utente denominato ELM_Access da utilizzare con i client JDBC e ODBC.

Gli utenti CA User Activity Reporting Module che dispongono delle autorizzazioni di accesso ai dati possono utilizzare ODBC o JDBC per accedere ai dati di evento. Ogni ruolo utente predefinito fornito con CA User Activity Reporting Module dispone delle suddette autorizzazioni. In questo esempio, è possibile creare un utente con qualsiasi ruolo di CA User Activity Reporting Module predefinito: Amministratore, Analista o Revisore.

Per creare il nuovo utente

1. Accedere al server CA User Activity Reporting Module come Amministratore.
2. Fare clic sulla scheda Amministrazione e sulla sottoscheda Gestione utenti e accessi.
3. Fare clic sul pulsante Utenti per visualizzare l'interfaccia utente CA EEM incorporata.
4. Fare clic su Nuovo utente. Verrà visualizzata la finestra di dialogo Nuovo utente.
5. Fare clic su Aggiungi informazioni su utente applicazione e assegnare all'account i privilegi di applicazione Amministratore.

   Nota: in un ambiente di produzione, all'utente vengono assegnati i permessi minimi per accedere ai dati. È possibile limitare l'accesso in molti modi, ad esempio tramite ruoli utente, criteri di accesso e filtri di accesso. Per ulteriori informazioni, consultare la *Guida in linea*.
6. Completare il record utente come necessario ed assegnare una password, prendendone nota per un successivo utilizzo.
7. Salvare l'utente e uscire dalla finestra Utenti.

Configurazione delle impostazioni del servizio ODBC

Utilizzare questa procedura per la configurazione delle impostazioni dei servizi ODBC e JDBC di CA User Activity Reporting Module.

Nota: le modifiche apportate in quest'area provocano un riavvio dei processi lato server che abilitano le comunicazioni ODBC e JDBC.

Per configurare il servizio ODBC

1. Accedere al server CA User Activity Reporting Module come utente amministratore.
2. Fare clic sulla scheda Amministrazione, quindi sulla sottoscheda Servizi.
3. Fare clic sul nodo Servizio ODBC.
4. Accettare le impostazioni predefinite:
   - Abilita servizio: True (consente le connessioni ODBC e JDBC sul server CA User Activity Reporting Module)
   - Porta 17002
   - Viene selezionato Crittografato (SSL)
   - Timeout sessione: 15 minuti
   - Livello di registrazione: accettare il valore predefinito, vale a dire NOTSET.
5. Fare clic su Salva.

Creazione di un'origine dati ODBC "elm"

Utilizzare questa procedura per creare un'origine dati denominata "CA-ELM."

Nota: installare il client OBDC prima di configurare l'origine dati.

Per creare un'origine dati

1. Accedere al Pannello di controllo di Windows.
2. Aprire la cartella Strumenti di amministrazione e avviare l'utilità Origini dati (ODBC).
3. Fare clic su Aggiungi per visualizzare la finestra di dialogo Crea nuova origine dati.
4. Selezionare la voce DataDirect OpenAccess SDK 6.0 e fare clic su Fine.

   L'utilità Driver Setup ODBC di DataDirect OpenAccess SDK visualizzerà una schermata di configurazione.
5. Immettere CA-ELM nel campo Nome origine dati e fornire una descrizione testuale.

6. Immettere il nome del server CA User Activity Reporting Module nel campo Host servizio. Questo esempio utilizza ca-elm.
7. Immettere 17002 nel campo Porta servizio.
8. Selezionare la casella di controllo Crittografia SSL.
9. Immettere le seguenti Proprietà personalizzate:

   ```
   querytimeout=600
   (seconds);queryfederated=true;queryfetchrows=1000;offsetmins=0;suppressNoncri
   ticalErrors=false
   ```

10. Fare clic su Applica, quindi su Verifica connessione.

    Se i parametri di connessione sono corretti, verrà visualizzato un messaggio di connessione riuscita.

11. Fare clic su OK per tornare alla finestra di dialogo Amministratore origine dati ODBC e quindi fare di nuovo clic su OK per uscire dall'utilità.

Considerazioni sull'origine dati ODBC

Seguono le descrizioni dei campi origine dati di ODBC relativi a CA User Activity Reporting Module:

Nome origine dati

Creare un nome per questa origine dati. Le applicazioni client che intendono utilizzare questi dati usano questo nome per connettersi all'origine dati.

Host di servizio

Specifica il nome del server CA User Activity Reporting Module a cui si connette il client. È possibile utilizzare sia un nome di host che un indirizzo IPv4.

Porta di servizio

Specifica la porta di servizio TCP su cui il server CA User Activity Reporting Module è in ascolto per le connessioni dei client ODBC. Il valore predefinito è 17002. Il valore impostato deve corrispondere all'impostazione del servizio Server ODBC. In caso contrario, si verificherà un errore di connessione.

Origine dati di servizio

Lasciare vuoto questo campo; in caso contrario, si verificherà un errore di connessione.

Crittografia SSL

Indica se utilizzare la crittografia per le comunicazioni fra il client ed il server CA User Activity Reporting Module. Il valore predefinito abilita la crittografia SSL. Il valore impostato deve corrispondere all'impostazione del servizio Server ODBC. In caso contrario, si verificherà un errore di connessione.

Proprietà personalizzate

Specifica le proprietà di connessione da utilizzare con l'archivio registro eventi. Il delimitatore delle proprietà è un punto e virgola senza spazi. I valori predefiniti consigliati sono i seguenti:

querytimeout

Indica il valore di timeout in secondi in assenza di dati restituiti, allo scadere del quale la query verrà chiusa. Segue la sintassi per questa proprietà:

```
querytimeout=300
```

queryfederated

Specifica se eseguire una query federata. Impostando questo valore su false, verrà eseguita una query solo sul server CA User Activity Reporting Module al quale viene eseguita la connessione di database. Segue la sintassi per questa proprietà:

```
queryfederated=true
```

queryfetchrows

Specifica il numero di righe da recuperare in una singola operazione, nel caso in cui la query abbia successo. Il valore minimo è 1 ed il massimo è 5000. Il valore predefinito è 1000. Segue la sintassi per questa proprietà:

```
queryfetchrows=1000
```

offsetmins

Specifica l'offset del fuso orario di questo client ODBC. Un valore pari a 0 utilizza il GMT. È possibile utilizzare questo campo per impostare il proprio offset di fuso orario rispetto al GMT. Segue la sintassi per questa proprietà:

```
offsetmins=0
```

suppressNoncriticalErrors

Indica il comportamento del provider di interfaccia in caso di errori non critici, ad esempio un database o un host che non rispondono.

Segue la sintassi per questa proprietà:

```
suppressNoncriticalErrors=false
```

Modifica del file di configurazione di Crystal Reports

Per poter utilizzare Crystal Reports con il client JDBC di CA User Activity Reporting Module, è innanzitutto necessario fornire alcune impostazioni di configurazione. Una volta configurato il file XML della configurazione di Crystal Reports, è possibile preparare ed inviare query ANSI SQL standard all'archivio di registro eventi CA User Activity Reporting Module.

Per configurare le impostazioni di Crystal Reports per JDBC

1. Accertarsi di copiare i file JAR del client JDBC sul server di Crystal Reports prima di modificare il file di configurazione.

   Ulteriori informazioni a riguardo sono disponibili nella *Guida all'implementazione*.

2. Accedere al server in cui si trova Crystal Reports.
3. Individuare il file CRConfig.xml ed aprirlo per modificarlo.
4. Individuare nel file il tag <DataDriverCommon> e la sezione del tag <Classpath> sottostante.
5. Aggiungere a classpath il percorso dei file JDBC JAR del client JDBC.
6. Modificare il valore nei tag dell'URL JDBC come segue:

   ```
   jdbc:ca-
   elm://127.0.0.1:17002;encrypted=1;ServerDataSource=Default;CustomProperties=(
   querytimeout=600;queryfederated=true;queryfetchrows=1000;offsetmins=0;suppres
   sNoncriticalErrors=false)
   ```

   Per ulteriori informazioni su questi parametri, consultare la sezione sulle considerazioni relative all'URL JDBC.

   Per ulteriori informazioni sull'impostazione dei parametri di connessione del prodotto, consultare la documentazione di Crystal Reports.

7. Modificare il valore nei tag Classname di JDBC come segue:

   ```
   com.ca.jdbc.openaccess.OpenAccessDriver
   ```

8. Salvare il file e uscire.

Ulteriori informazioni:

Considerazioni sull'URL JDBC (a pagina 710)

Considerazioni sull'URL JDBC

Quando si utilizza il client JDBC per accedere ai dati evento archiviati in CA User Activity Reporting Module, sono necessari sia il classpath che l'URL JDBC. Il Classpath JDBC indica il percorso dei file JAR del driver. L'URL JDBC definisce i parametri utilizzati dalle classi dei file JAR durante il caricamento.

Segue un completo URL JDBC campione:

```
jdbc:ca-
elm://127.0.0.1:17002;encrypted=1;ServerDataSource=Default;CustomProperties=(querytimeout=600;que
ryfederated=true;queryfetchrows=1000;offsetmins=0;suppressNoncriticalErrors=false)
```

Di seguito sono descritti i componenti dell'URL:

jdbc.ca-elm:

Definisce la stringa protocol:subprotocol che indica il driver JDBC fornito con CA User Activity Reporting Module.

//IP Address:Port;

Indica l'indirizzo IP che rappresenta il server CA User Activity Reporting Module contenente i dati ai quali si desidera accedere. Il numero di porta è la porta da utilizzare per le comunicazioni e deve corrispondere all'impostazione configurata nel riquadro Servizio ODBC di CA User Activity Reporting Module. Se le porte non trovano corrispondenza, si verificherà un errore nel tentativo di connessione.

encrypted=0|1;

Stabilisce se si utilizza la crittografia SSL per le comunicazioni tra il client JDBC ed il server CA User Activity Reporting Module. Il valore predefinito è 0, non crittografato, e non è necessario specificarlo nell'URL. L'impostazione encrypted=1 consente di attivare la crittografia. Impostare la connessione sulla crittografia in modo esplicito. Inoltre, tale impostazione deve corrispondere a quanto configurato nella finestra di dialogo del Servizio ODBC CA User Activity Reporting Module; in caso contrario, si verificherà un errore di connessione.

ServerDataSource=Default

Specifica il nome dell'origine dati. Impostare questo valore su *Default* per accedere all'archivio registro eventi di CA User Activity Reporting Module.

CustomProperties=(x;y;z)

Queste proprietà sono identiche alle proprietà di ODBC personalizzate. Se non vengono specificate esplicitamente, verranno applicati i valori predefiniti visualizzati nell'URL di esempio.

Ulteriori informazioni

Considerazioni sull'origine dati ODBC (a pagina 707)

Esempio di creazione eventi per ODBC

Per visualizzare la query di esempio, creare alcuni eventi rilevanti causando attività con errori come le seguenti:

- Eseguire più volte l'accesso al server CA User Activity Reporting Module in modo errato.
- Eseguire l'accesso in modo errato ad un host agente i cui eventi sono diretti a un server CA User Activity Reporting Module specifico.
- Accedere alle risorse di rete o sistema immettendo le credenziali errate.

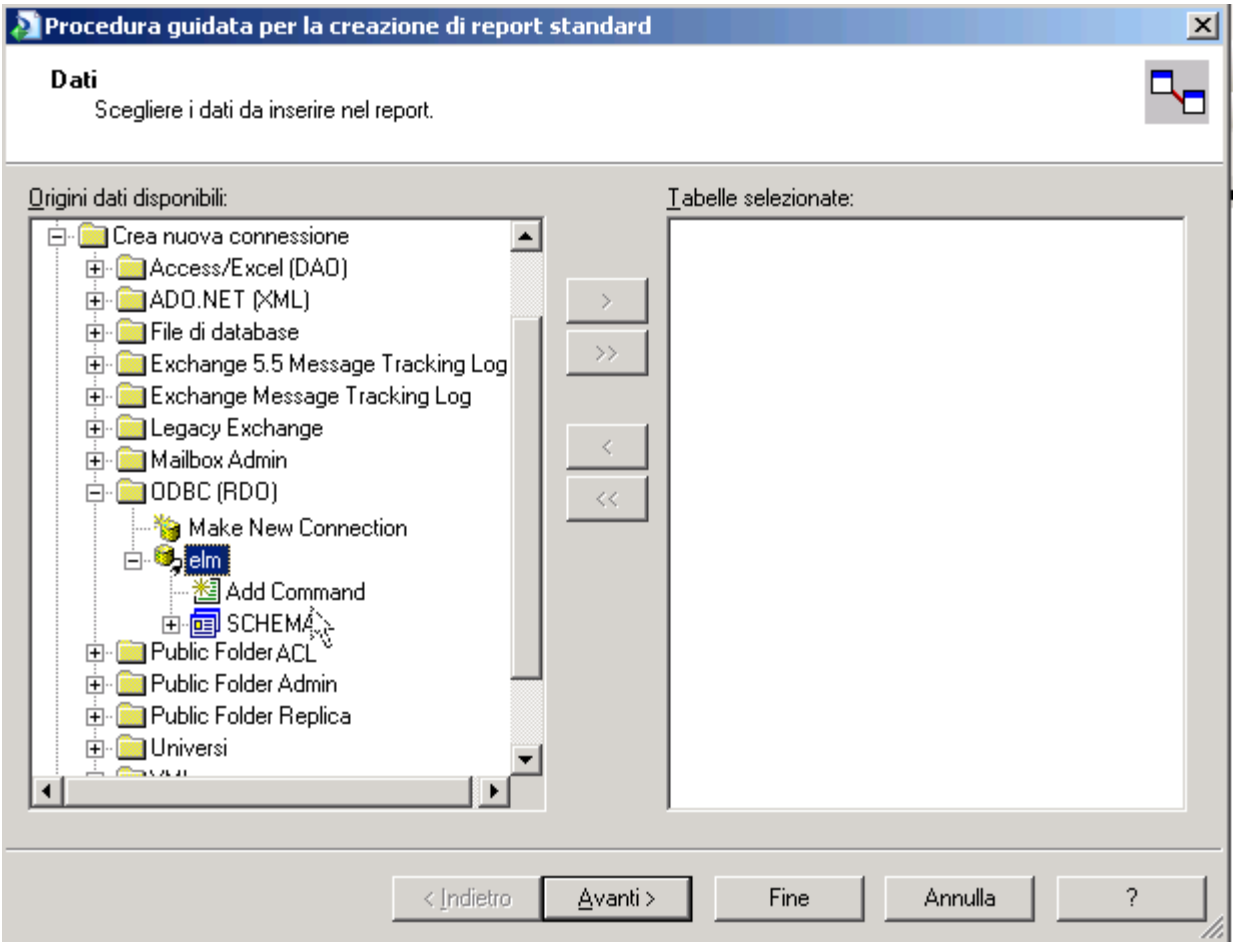
Utilizzare Crystal Reports per accedere all'Archivio di registro eventi con ODBC

È possibile utilizzare la funzionalità di accesso ODBC per interrogare i dati di evento CA User Activity Reporting Module da uno strumento di rapporti di terze parti come BusinessObjects Crystal Reports. Al termine dell'installazione e delle configurazioni necessarie, si è pronti per preparare e inviare query ANSI SQL standard all'archivio di registro eventi di CA User Activity Reporting Module.

Lo schema di database dell'archivio di registro eventi è la grammatica evento comune (CEG). La guida in linea di CA User Activity Reporting Module contiene un componente CEG di riferimento che aiuta l'utente nella creazione delle query. È inoltre possibile consultare le istruzioni SQL sottostanti delle query in dotazione, ma per accedere al database dall'esterno di CA User Activity Reporting Module è necessario utilizzare ANSI SQL.

Per accedere ai dati evento da Crystal Reports

1. Completare le attività necessarie di installazione e configurazione.
2. Avviare Crystal Reports e accedere alla procedura guidata Rapporti standard.
3. Creare una connessione ODBC nella finestra di dialogo Dati e selezionare l'origine dati ODBC precedentemente creata nel Pannello di controllo di Windows.



4. Utilizzare la funzionalità Aggiungi comando per creare una query nell'area SQL.

   Ad esempio, è possibile creare la query seguente:

   ```
   SELECT source_username as source_username , SUM(event_count) AS
   FUNC_SUM_event_count FROM view_event WHERE  event_result = 'F' GROUP BY
   source_username ORDER BY FUNC_SUM_event_count DESC;
   ```

5. Fare clic su OK per completare l'immissione della query.

   Verrà visualizzato un modello di rapporto in cui inserire le colonne di dati restituite dalla query.

6. Trascinare i campi dallo strumento di esplorazione campi, nell'angolo in alto a destra, nel modello di rapporto in formato di colonne.

   L'esecuzione della query visualizza i valori associati ai campi. È possibile utilizzare Crystal Reports per creare tutte le visualizzazioni o personalizzazioni necessarie.

7. (Facoltativo) Confrontare i risultati del rapporto con il rapporto in dotazione "Attività non riuscite per Esecutore".

Accesso a Eventi da Crystal Reports con JDBC

Le seguenti attività consentono di utilizzare JDBC per accedere all'archivio di registro eventi:

1. Copiare i file JDBC JAR del client sul server in cui si trova Crystal Reports.
2. Modificare il file di configurazione di Crystal Reports.
3. Utilizzare Crystal Reports per inviare una query.

Nota: questo processo e gli esempi correlati presuppongono che l'utente abbia acquisito familiarità con la creazione di istruzioni SQL di base e l'utilizzo di Crystal Reports. Ulteriori informazioni sull'utilizzo di Crystal Reports sono disponibili nella guida in linea di BusinessObjects.

Copiare i file JAR del driver JDBC

Prima di utilizzare il driver JDBC per accedere agli eventi da un server CA User Activity Reporting Module, copiare i file JAR sul server dal quale eseguire l'accesso.

Per copiare i file

1. Aprire l'immagine ISO oppure accedere al DVD di installazione dell'applicazione.
2. Individuare la directory \CA\ELM\JDBC.
3. Copiare i file JAR sul server in cui si trova Crystal Reports.

   Il pacchetto del rapporto utilizzato richiede una posizione specifica per i file. Consultare la documentazione fornita con l'applicazione.
4. Quando si configurano le connessioni, annotare la directory in cui sistemare i file per il percorso di riferimento.

Utilizzare Crystal Reports per accedere all'Archivio registro eventi con JDBC

La funzione di accesso JDBC può essere utilizzata per interrogare i dati dell'evento CA User Activity Reporting Module da uno strumento per la creazione di rapporti di terze parti come BusinessObjects Crystal Reports.

Lo schema di database dell'archivio di registro eventi è la grammatica evento comune (CEG). La guida in linea di CA User Activity Reporting Module contiene un componente CEG di riferimento che aiuta l'utente nella creazione delle query. È inoltre possibile consultare le istruzioni SQL sottostanti delle query in dotazione, ma per accedere al database dall'esterno di CA User Activity Reporting Module è necessario utilizzare ANSI SQL.

Per accedere ai dati evento da Crystal Reports

1. Avviare Crystal Reports e accedere alla procedura guidata Rapporti standard.
2. Nella finestra di dialogo Dati, creare una connessione JDBC.

   Nota:quando viene visualizzata la finestra Informazioni di connessione, utilizzare il valore *Default* per il nome del database.
3. Utilizzare la funzionalità Aggiungi comando per creare ed eseguire la seguente query nell'area della voce SQL:

   ```
   SELECT source_username as source_username , SUM(event_count) AS
   FUNC_SUM_event_count FROM view_event WHERE  event_result = 'F' GROUP BY
   source_username ORDER BY FUNC_SUM_event_count DESC;
   ```

4. Trascinare i campi da Esplora campo riportato sulla destra nelle colonne del modello.

   L'esecuzione della query visualizza i valori associati ai campi. Gli strumenti di Crystal Reports possono essere utilizzati per creare qualsiasi visualizzazione o personalizzazione necessaria.

5. (Facoltativo) Confrontare i risultati del rapporto con il rapporto in dotazione "Attività non riuscite per Esecutore".

Eliminare il client ODBC sui sistemi Windows

Su tutte le piattaforme Windows, la funzione Elimina del pacchetto di installazione del client consente di eliminare i file di prodotto e le voci nelle informazioni di sistema.

Importante: Creando file di origine IP nella directory di installazione locale del client ODBC, eseguire una copia di backup dei file in una posizione diversa prima di eliminare il client ODBC dal sistema Windows.

Se il client ODBC locale è installato e si desidera modificare la posizione di installazione, utilizzare l'opzione Elimina. Eliminare il client locale ODBC installato e reinstallarlo nella nuova posizione.

Per eliminare il client ODBC

1. Accedere all'utilità Programmi e funzionalità nel pannello di controllo di Windows
2. Individuare e selezionare la voce Driver ODBC di CA User Activity Reporting Module.
3. Fare clic su Rimuovi.

Rimozione del client JDBC

Per disinstallare il client JDBC, rimuovere la directory di installazione.

Glossario

accesso dati

Accesso dati è un tipo di autorizzazione conferita a tutti i CA User Activity Reporting Module sfruttando il Criterio predefinito di accesso ai dati., nella classe di risorsa di CALM. Ogni utente può accedere a tutti i dati, a meno che non lo si impedisca mediante dei filtri di accesso.

Accesso ODBC e JDBC

L'*accesso ODBC e JDBC* agli archivi di registro eventi di CA User Activity Reporting Module supporta l'utilizzo dei dati di evento con svariati prodotti di terze parti, inclusa la creazione di rapporti eventi personalizzati con strumenti di terze parti, la correlazione di eventi mediante motori di correlazione e la valutazione degli eventi tramite prodotti per il rilevamento di violazioni o malware. I sistemi Windows utilizzano l'accesso ODBC; i sistemi UNIX e LINUX utilizzano l'accesso JDBC.

account

Un *account* è un utente globale che è anche un utente dell'applicazione CALM. Un singolo individuo può disporre di più di un account, ognuno dei quali dotato di un diverso ruolo definito dall'utente.

adapter CA

Gli *adapter CA* sono un gruppo di listener che riceve eventi da componenti di CA Audit come i client di CA Audit e i recorder iRecorder e SAPI, oltre ad essere le origini che inviano nativamente gli eventi con iTechnology.

agente

Un *agente* è un servizio generico configurato con dei connettori, ognuno dei quali raccoglie eventi non elaborati da una singola origine evento per poi inviarli a CA User Activity Reporting Module per l'elaborazione. Ogni CALM> è dotato di un agente integrato. Inoltre, è possibile installare un agente su un punto di raccolta remoto e raccogliere gli eventi negli host in cui non si possono installare agenti. È possibile anche installare un agente su un host in cui si eseguono le origini evento, e poter quindi applicare le regole di soppressione e crittografare la trasmissione a CA User Activity Reporting Module.

agente predefinito

L'*agente predefinito* è l'agente che viene installato con il server CA User Activity Reporting Module. Può essere configurato per la raccolta diretta di eventi syslog nonché per la raccolta da diverse origini eventi non syslog come CA Access Control r12 SP1, Servizi di certificazione Microsoft Active Directory e database Oracle9i.

aggiornamenti di contenuto

Gli aggiornamenti di contenuto sono le parti non binarie degli aggiornamenti di sottoscrizione salvati nel server di gestione CA User Activity Reporting Module. Gli aggiornamenti di contenuto comprendono contenuti come i file XMP e DM, gli aggiornamenti di configurazione per i moduli di CA User Activity Reporting Module e gli aggiornamenti della chiave pubblica.

aggiornamenti di sottoscrizione

Gli aggiornamenti di sottoscrizione sono i file binari e non, distribuiti dal server di sottoscrizione diCA. I file binari sono degli aggiornamenti di modulo di prodotto solitamente installati sui CA User Activity Reporting Module. I file non binari, o aggiornamenti di contenuto, vengono memorizzati sul server di gestione.

aggregazione evento

L'aggregazione evento è il processo di consolidamento delle voci di registro simili fra loro in una singola voce contenente il numero di ricorrenze dell'evento. Le regole di riepilogo definiscono la modalità di aggregazione degli eventi.

analisi

L'analisi, detta anche analisi del messaggio, è il processo di acquisizione dei dati non elaborati di dispositivo allo scopo di trasformarli in coppie chiave-valore. L'analisi si esegue usando un file XMP. L'analisi, che precede il mapping dei dati, è un passo del procedimento di integrazione, che trasforma gli eventi non elaborati raccolti da un'origine evento in un evento perfezionato che si può visualizzare.

analisi dei file XMP

L'analisi dei file XMP è il procedimento eseguita dall'utility di Analisi del messaggio per individuare tutti gli eventi contenenti ogni stringa di corrispondenza preliminare. Si dividerà quindi ogni evento corrispondente in token in modo da poterlo analizzare utilizzando il primo filtro individuato che utilizzi la medesima stringa di corrispondenza preliminare.

analisi del mapping

L'*analisi del mapping* è un passaggio nella procedura guidata File di mapping che consente di verificare ed eseguire delle modifiche ad un file di mapping dei dati. Gli eventi campione vergono verificati tramite il file di mapping dei dati, ed i risultati si convalidano con la CEG.

analisi di messaggio

L'analisi di messaggio è il processo di applicazione delle regole all'analisi di un registro di eventi non elaborati, in modo da ottenere informazioni specifiche come il timestamp, l'indirizzo IP ed il nome utente. Le regole di analisi utilizzano la corrispondenza dei caratteri per individuare un preciso testo di evento e collegarlo ai valori selezionati.

analisi di registro

L'analisi di registro è il procedimento di estrazione dei dati da un registro, in modo che i valori analizzati possano essere utilizzati in una fase successiva della gestione di registro.

analisi di registro

L'analisi di registro è lo studio delle voci di registro utile per identificare gli eventi d'interesse. Se i registri non vengono analizzati in maniera tempestiva, il loro valore si riduce significativamente.

applicazione software

Un'*applicazione software*è un pacchetto software completamente funzionante contenente il software, il sistema operativo sottostante ed i relativi pacchetti. L'avvio del supporto di installazione consente di installare l'applicazione sull'hardware fornito dall'utente finale.

AppObject

Gli *AppObject,* o oggetti applicazione, sono risorse specifiche di prodotto memorizzate in CA EEM sotto l'istanza applicazione di un dato prodotto. Per l'istanza applicazione di CAELM, tali risorse comprendono i contenuti di rapporto e di query, le attività pianificate per i rapporti e gli avvisi, i contenuti e le configurazioni degli agenti, le configurazioni di servizi, adapter ed integrazioni, i file di mapping dei dati e di analisi del messaggio e le regole di soppressione e di riepilogo.

archiviazione automatica

L'archiviazione automatica è un procedimento configurabile che consente di automatizzare lo spostamento dei database di archivio da un server all'altro. Nella prima fase dell'archiviazione automatica, il server di raccolta invia al server di rapporto i database appena archiviati, ad intervalli specificati dall'utente. Nella seconda fase, il server di rapporto invia i database invecchiati al server di archiviazione remota per archiviarli a lungo termine, eliminando così la necessità di eseguire un backup manuale e la procedura di spostamento. Per eseguire un'archiviazione automatica, l'utente dovrà configurare un'autenticazione priva di password dal server di origine a quello di destinazione.

archiviazione di registro

L'archiviazione di registro è il processo che si verifica quando il database hot raggiunge le sue dimensioni massime, pur avendo eseguito la compressione di riga e dopo aver cambiato stato da hot a warm. Gli amministratori devono eseguire manualmente un backup dei database warm prima che sia raggiunta la soglia di eliminazione, oltre a dover eseguire l'utility LMArchive per registrare il nome dei backup. Archivia query consentirà quindi di visionare questa informazione.

archivio di catalogo

Consultare il catalogo.

archivio registro eventi

L'*archivio registro eventi* è un componente del server CA User Activity Reporting Module in cui gli eventi in arrivo si archiviano nei database. Occorre creare manualmente un backup dei database dell'archivio registro eventi, per poi spostarli su una soluzione remota di archiviazione dei registri prima dell'ora stabilita per l'eliminazione. È possibile ripristinare i database archiviati in un archivio registro eventi.

archivio registro eventi

L'archivio registro eventi è il risultato del processo di archiviazione, in cui l'utente esegue il backup di un database warm ed invia una notifica a CA User Activity Reporting Module con l'utility LMArchive. Fatto ciò, il database sottoposto a backup passerà dall'archivio registro eventi all'archivio a lungo termine.

archivio utente

Un *archivio utente* è il repository delle informazioni utente e dei criteri di password globali. Per impostazione predefinita, l'archivio utente di CA User Activity Reporting Module è il repository locale. È possibile anche configurarlo in modo da fare riferimento a CA SiteMinder o ad una directory LDAP supportata come Microsoft Active Directory, Sun One o Novell eDirectory. Indipendentemente dal modo in cui si configura l'archivio utente, il repository locale sul server di gestione contiene informazioni specifiche di applicazione sugli utenti, come ad esempio il ruolo utente e i criteri di accesso associati.

Autenticazione ssh non interattiva

L'autenticazione *non interattiva*abilita lo spostamento dei file da un server all'altro senza dover immettere una passphrase per l'autenticazione. Impostare l'autenticazione non interattiva dal server di origine al server di destinazione prima di configurare l'archiviazione automatica o di utilizzare lo script restore-ca-elm.sh.

avviso

Un *avviso* è un processo pianificato di query che è possibile utilizzare per individuare le violazioni di criterio, le tendenze di utilizzo, gli schemi di accesso e le altre informazioni che richiedono attenzione a breve termine. Per impostazione predefinita, quando la query di avviso restituisce risultati, essi verranno visualizzati nella pagina degli avvisi di CA User Activity Reporting Module e quindi aggiunti ad un feed RSS. Quando si pianifica un avviso, è possibile specificare destinazioni aggiuntive, come ad esempio la posta elettronica, un processo CA IT PAM di output di evento/avviso e i trap SNMP.

CA Enterprise Log Manager

CA User Activity Reporting Module è una soluzione utile per raccogliere i registri da origini evento di tipi diversi ed ampiamente distribuite, per verificare la conformità con le query e con i rapporti e per tener traccia dei database di registri compressi trasferiti su soluzioni esterne di archiviazione a lungo termine.

CA IT PAM

CA IT PAM corrisponde alla forma abbreviata di CA IT Process Automation Manager. Questo prodotto CA automatizza i processi definiti dall'utente. CA User Activity Reporting Module utilizza due processi: la creazione di un processo di output evento/avviso per un prodotto locale, come CA Service Desk, ed il processo di creazione dinamica di elenchi che possono essere importati come valori chiave. Per eseguire l'integrazione, è necessario disporre di CA IT PAM r2.1.

CA Spectrum

CA Spectrum è un prodotto di gestione degli errori di rete che è possibile integrare con CA User Activity Reporting Module per l'utilizzo come destinazione di avvisi inviati sottoforma di trap SNMP.

CAELM

CAELM è il nome di istanza applicazione che CA EEM utilizza per CA User Activity Reporting Module. Per accedere alle funzionalità di CA User Activity Reporting Module di CA Embedded Entitlements Manager, inserire l'URL https://<ip_address>:5250/spin/eiam/eiam.csp, selezionare CAELM come nome di applicazione, ed inserire la password dell'utente EiamAdmin.

caelmadmin

Il nome utente e la password di *caelmadmin* sono credenziali necessarie per accedere al sistema operativo dell'applicazione software. L'ID utente caelmadmin viene creato durante l'installazione di questo sistema operativo. Durante l'installazione del componente software, l'installatore deve specificare la password di EiamAdmin, ovvero dell'account di super utente di CA EEM. La stessa password verrà assegnata anche all'account caelmadmin. Si consiglia all'amministratore del server di accedere via ssh come utente caelmadmin, e di modificare la password predefinita. Anche se l'amministratore non può accedere via ssh come utente principale, potrà passare gli utenti all'account principale con il relativo comando (su root).

caelmservice

caelmservice è un account di servizio utile per eseguire iGateway ed i servizi locali di CA EEM come utente non principale. L'account caelmservice si utilizza per installare gli aggiornamenti del sistema operativo scaricati insieme agli aggiornamenti di sottoscrizione.

calendario

Un *calendario* consente di limitare il tempo di effettiva applicazione di un criterio d'accesso. Un criterio consente alle identità specificate di eseguire azioni su una risorsa in un certo periodo di tempo.

CALM

CALM è una classe di risorsa predefinita che comprende le seguenti risorse di CA User Activity Reporting Module: avviso, ArchiveQuery, calmTag, dati, EventGrouping, integrazione e rapporto. Le azioni consentite su questa classe di risorsa sono Annotazione (rapporti), Creazione (avviso, calmTag, EventGrouping, integrazione e rapporto), Dataaccess (Dati), Esecuzione (ArchiveQuery) e Pianificazione (avviso, rapporto).

calmTag

calmTag è un attributo di AppObject dotato di nome, che si utilizza creando un criterio di scoping per limitare gli utenti all'utilizzo di rapporti e query appartenenti a determinati tag. Tutti i rapporti e le query sono AppObject, e possono avere calmTag come attributo (non si deve confondere con il tag risorsa).

Campi CEG

I campi CEG sono etichette utilizzate per standardizzare la presentazione dei campi di eventi non elaborati provenienti da diverse origini evento. Durante il perfezionamento degli eventi, CA User Activity Reporting Module analizza i messaggi degli eventi non elaborati ottenendo una serie di coppie nome/valore e mappa i nomi degli eventi non elaborati ai campi CEG standard. Questo perfezionamento crea delle coppie nome/valore che consistono in campi e valori CEG provenienti dall'evento non elaborato. In altre parole, quando si perfezionano gli eventi non elaborati, le diverse etichette utilizzate in essi per lo stesso oggetto dati o elemento di rete vengono convertiti allo stesso nome di campo CEG. I campi CEG verranno mappati agli OID nella MIB utilizzata per i trap SNMP.

cartella

Una *cartella* è la posizione di un percorso di directory utilizzati dal server di gestione CA User Activity Reporting Module per memorizzare i tipi oggetto di CA User Activity Reporting Module. Nei criteri di scoping è possibile far riferimento alle cartelle per consentire o negare agli utenti di accedere ad un tipo di oggetto specifico.

catalogo

Il *catalogo* è il database in cui ogni CA User Activity Reporting Module conserva lo stato dei database archiviati, agendo anche come un indice di alto livello su tutti i database. Le informazioni di stato (warm, cold o defrosted) verranno mantenute per tutti i database presenti in questo CA User Activity Reporting Module e per qualsiasi altro database ripristinato in questo CA User Activity Reporting Module come defrosted. Le funzionalità di indicizzazione si estendono a tutti i database hot e warm nell'archivio registro eventi di questo CA User Activity Reporting Module.

categorie di evento

Le categorie di evento sono i tag utilizzati da CA User Activity Reporting Module per classificare gli eventi in base alla loro funzione, prima di inserirli nell'archivio eventi.

certificati

I *certificati* predefiniti utilizzati da CA User Activity Reporting Module sono CAELMCert.cer e CAELM_AgentCert.cer. Tutti i servizi CA User Activity Reporting Module utilizzano CAELMCert.cer per la comunicazione con il server di gestione. Tutti gli agenti utilizzano CAELM_AgentCert.cer per la comunicazione con i server di raccolta.

client di sottoscrizione

Un *client di sottoscrizione* è un server CA User Activity Reporting Module in grado di ottenere aggiornamenti di contenuto da un altro server CA User Activity Reporting Module, denominato server proxy di sottoscrizione. I client di sottoscrizione sondano regolarmente i server proxy di sottoscrizione configurati, e prelevano i nuovi aggiornamenti quando sono disponibili. Dopo aver prelevato gli aggiornamenti, il client installa i componenti scaricati.

Compatibile con FIPS 140-2

Compatibile con FIPS 140-2 designa un prodotto che può utilizzare *facoltativamente* librerie di crittografia conformi a FIPS ed algoritmi per crittografare e decrittografare dati sensibili. CA User Activity Reporting Module è una prodotto di raccolta di log compatibili con FIPS; è infatti possibile scegliere l'esecuzione in modalità FIPS o Non FIPS.

componenti di visualizzazione

I componenti di visualizzazione sono opzioni utili per visualizzare i dati di rapporto fra cui una tabella, un diagramma (a linee, a barre, a colonne e a torta), oppure un visualizzatore eventi.

configurazione globale

La *configurazione globale* è una serie di impostazioni che si applica a tutti i serverCA User Activity Reporting Module che utilizzano il medesimo server di gestione.

configurazione salvata

Una *configurazione salvata* è una configurazione archiviata con i valori degli attributi di accesso ai dati di un'integrazione, che si può utilizzare come modello per creare una nuova integrazione.

Conforme a FIPS 140-2

Conforme a FIPS 140-2 designa un prodotto che, per impostazione predefinita, utilizza *solo* algoritmi di crittografia certificati da un laboratorio accreditato di verifica dei moduli crittografici (CMT, Cryptographic Module Testing). CA User Activity Reporting Module può utilizzare moduli crittografici basati sulle librerie certificate BSAFE Crypto-C ME e Crypto-J libraries RSA in modalità FIPS. Solitamente, non si tratta tuttavia dell'impostazione predefinita.

connettore

Un *connettore* è un'integrazione per una particolare origine evento configurata su un dato agente. Un agente può caricare in memoria più connettori, di tipi simili o diversi. Il connettore consente la raccolta degli eventi non elaborati da un'origine e la trasmissione basata su regole degli eventi convertiti verso un archivio registro eventi, in cui essi saranno inseriti in un database hot. Le integrazioni out-of-the-box offrono una raccolta ottimizzata di una vasta gamma di origini evento, compresi i sistemi operativi, i database, i server Web, i firewall e molti altri tipi di applicazioni di protezione. È possibile definire un connettore per una propria origine evento da zero, oppure utilizzare un'integrazione come modello.

Contenuto dei trap SNMP

Un *trap SNMP* consiste in una serie di coppie nome/valore, in cui ogni nome è un OID (identificatore oggetto) ed ogni valore viene restituito da un avviso pianificato. I risultati di query restituiti da un avviso sono costituiti dai campi CEG e relativi valori. Il trap SNMP viene popolato sostituendo un OID per ogni campo CEG utilizzato per il nome della coppia nome/valore. La mappatura di ogni campo CEG a un OID viene memorizzata nella MIB. Il trap SNMP comprende solo le coppie nome/valore per i campi selezionati al momento di configurare l'avviso.

criterio di accesso

Un *criterio di accesso* è una regola che conferisce o nega ad un'identità (utente o gruppo utente) i diritti di accesso ad una risorsa applicazione. CA User Activity Reporting Module stabilisce se i criteri siano applicabili ad un utente specifico facendo corrispondere identità, risorse e classi di risorse, e valutando i filtri.

Criterio di accesso all'applicazione CALM

Il *Criterio di accesso all'applicazione CALM* è un tipo di elenco di controllo di accesso di un criterio di scoping che definisce chi può accedere a CA User Activity Reporting Module. Per impostazione predefinita, l'amministratore [di gruppo], l'analista [di gruppo] ed il revisore [di gruppo] potranno eseguire l'accesso.

criterio di delega

Un *criterio di delega* è un criterio di accesso che consente ad un utente di delegare la propria autorità ad un altro utente o ad un gruppo applicazione, globale o dinamico. È necessario eliminare esplicitamente i criteri di delega creati dall'utente eliminato o disattivato.

criterio di obbligo

Un *criterio di obbligo* è un criterio creato automaticamente insieme ad un filtro di accesso. Non si dovrebbe provare a creare, a modificare o ad eliminare direttamente un criterio di obbligo. Si consiglia invece di creare, di modificare o di eliminare il filtro d'accesso.

criterio di scoping

Un *criterio di scoping* è un tipo di criterio di accesso che conferisce o nega l'accesso alle risorse memorizzate nel server di gestione, come ad esempio AppObjects, utenti, gruppi, cartelle e criteri. Un criterio di scoping stabilisce quali identità possano accedere alle risorse specificate.

database archiviati

I *database archiviati* su un dato server CA User Activity Reporting Module comprendono tutti i database warm disponibili per le query per cui è necessario eseguire un backup manuale prima della scadenza, tutti i database cold registrati come sottoposti a backup e tutti quelli registrati come ripristinati dal backup.

defrosting

Il defrosting è il procedimento di modifica dello stato di un database da cold a defrosted. Questo processo viene eseguito da CA User Activity Reporting Module quando viene ricevuta una notifica dll'utility LMArchive relativa all'avvenuto ripristino di un database cold noto (se non si ripristina il database cold nel suo CA User Activity Reporting Module originale, non si dovrà utilizzare LMArchive ed eseguire il defrosting; con la ricatalogazione si aggiungerà il database ripristinato come database warm).

Destinazioni di trap SNMP

Quando si pianifica un avviso è possibile aggiungere una o più *destinazioni di trap SNMP*. Ogni destinazione di trap SNMP viene configurata con un indirizzo IP ed una porta. La destinazione è di solito un NOC o un server di gestione, come CA Spectrum o CA NSM. Quando le query per un processo di avviso pianificato restituiscono risultati verrà inviato un trap SNMP alle destinazioni configurate.

elementi di integrazione

Gli elementi di integrazione comprendono un sensore, un assistente di configurazione, un file di accesso dati ed uno o più file di analisi del messaggio (XMP) e di mapping dei dati.

elenco controllo di accesso identità

Un *elenco controllo di accesso identità* consente di specificare le diverse azioni che ogni identità selezionata può eseguire sulle risorse selezionate. Ad esempio, con un elenco di controllo accesso identità si può fare in modo che un'identità possa creare rapporti ed un'altra possa pianificarli ed annotarli. Un elenco controllo di accesso identità differisce da un elenco di controllo di accesso nel fatto che esso è incentrato sull'identità piuttosto che sulla risorsa.

event_action

event_action è il campo specifico di evento di quarto livello nella normalizzazione degli eventi utilizzata dalla CEG. Esso descrive azioni comuni. Avvio processo, Arresto processo ed Errore applicazione sono alcuni esempi di tipi di azioni evento.

event_category

event_category è il campo specifico di evento di secondo livello nella normalizzazione degli eventi utilizzata dalla CEG. Esso consente un'ulteriore classificazione degli eventi con uno specifico ideal_model. Alcuni tipi di categoria evento: Sicurezza operativa, Gestione identità, Gestione configurazione, Accesso alla risorsa e Accesso al sistema.

event_class

event_class è il campo specifico di evento di terzo livello nella normalizzazione degli eventi utilizzata dalla CEG. Esso consente un'ulteriore classificazione degli eventi in una specifica event_category.

eventi

Gli eventi in CA User Activity Reporting Module sono i record di registro generati da ogni origine evento specificata.

evento di automonitoraggio

Un *evento di automonitoraggio* è un evento registrato da CA User Activity Reporting Module. Le azioni eseguite dagli utenti entrati nel sistema, e le funzioni eseguite da diversi moduli, come i servizi e i listener, genereranno automaticamente questo tipo di eventi. È possibile visualizzare il rapporto di Dettagli eventi di automonitoraggio operazioni SIM selezionando un server di rapporto ed aprendo la scheda Eventi di automonitoraggio.

evento di osservazione

Un *evento di osservazione* è un evento che coinvolge un'origine, una destinazione ed un agente, in cui un agente di raccolta evento osserva e registra l'evento.

evento locale

Un *evento locale* è un evento che coinvolge una singola entità, in cui il medesimo host costituisce l'origine e la destinazione dell'evento. Un evento locale è il primo dei quattro tipi di evento utilizzati nella Grammatica evento comune.

evento nativo

Un *evento nativo* è lo stato o l'azione che attiva un evento non elaborato. È possibile ricevere ed analizzare o mappare gli eventi nativi come appropriato, per poi trasmetterli sotto forma di eventi perfezionati o non elaborati. Una mancata autenticazione è un evento nativo.

evento non elaborato

Un *evento non elaborato* è un'informazione attivata da un evento nativo inviata da un agente di monitoraggio al Log Manager collector. L'evento non elaborato viene spesso formattato come stringa syslog o come coppia nome-valore. In CA User Activity Reporting Module è possibile rivedere un evento nella sua forma non elaborata.

evento perfezionato

Un *evento perfezionato* è un'informazione evento mappata o analizzata che deriva da eventi non elaborati o riepilogati. CA User Activity Reporting Module esegue il mapping e l'analisi in modo che sia possibile ricercare le informazioni archiviate.

evento registrato

Si definiscono *evento registrato* le informazioni di evento non elaborate o perfezionate già inserite in un database. Gli eventi non elaborati vengono sempre registrati, a meno che non li si elimini o li si riepiloghi come avviene per gli eventi perfezionati. Si tratta di informazioni memorizzate e ricercabili.

evento remoto

Un *evento remoto* è un evento che coinvolge due diversi computer host, ovvero l'origine e la destinazione. Un evento remoto è il secondo dei quattro tipi di evento utilizzati nella Grammatica evento comune.

evento RSS

Un *evento RSS* è un evento generato da CA User Activity Reporting Module per convogliare un avviso verso prodotti ed utenti di terze parti. L'evento è un riepilogo del risultato di ogni avviso, ed un collegamento al file di risultato. È possibile configurare la durata di un dato elemento del feed RSS.

explorer agente

Explorer agente è l'archivio delle impostazioni di configurazione degli agenti (gli agenti si possono installare su un punto di raccolta o sugli endpoint in cui esistono delle origini evento).

federazione a coppie

Una *federazione a coppie* di server CA User Activity Reporting Module è una topologia che definisce una relazione paritaria fra server. Nella sua forma più semplice, il server 2 è figlio del server 1, ed il server 1 è figlio del server 2. Fra queste coppie di server vige una relazione a doppio senso. Si può definire una federazione a coppie per fare in modo che molti server siano peer l'uno dell'altro. Una query federata restituisce risultati dal server selezionato e da tutti i suoi peer.

federazione gerarchica

Una *federazione gerarchica* di server CA User Activity Reporting Module è una topologia che definisce una relazione gerarchica fra server. Nella sua forma più semplice, il server 2 è figlio del server 1, ma il server 1 non è figlio del server 2. Cioè, la relazione è a senso unico. Una federazione gerarchica può sfruttare più livelli di relazioni padre-figlio, mentre un singolo server padre può avere diversi server figlio. Una query federata produrrà risultati dai server selezionati e dai relativi figli.

file di analisi del messaggio (XMP)

Un *file di analisi del messaggio (XMP)* è un file XML, associato ad un tipo specifico di origine evento, che applica le regole di analisi. Le regole di analisi suddividono i dati rilevanti in un evento non elaborato in coppie nome-valore, che si potranno inviare al file di mapping dei dati per eseguire ulteriori elaborazioni. Questo tipo di file si utilizza in tutte le integrazioni e nei connettori, che si basano su di esse. Nel caso degli adapter CA, i file XMP si possono applicare anche al server CA User Activity Reporting Module.

file di mapping dei dati (DM)

I file di mapping dei dati (DM) sono file XML che utilizzano la Grammatica evento comune (CEG) di CA per trasformare gli eventi da un formato di origine ad uno conforme alla CEG, che sia possibile memorizzare nell'Archivio registro eventi a scopo di analisi e di creazione di rapporti. Ogni nome di registro deve disporre di un file DM prima di poter memorizzare i dati evento. Gli utenti possono modificare la copia di un file DM ed applicarla ad un determinato connettore.

filtraggio degli eventi

Il filtraggio degli eventi è il processo di rimozione degli eventi basato sui filtri di CEG.

filtro

Un *filtro* consente di porre dei limiti ad una query di archivio registro eventi.

filtro di accesso

Un *filtro di accesso* è un filtro che l'amministratore può impostare per controllare quali dati evento possano essere visualizzati dagli utenti e dai gruppi non amministrativi. Ad esempio, un filtro di accesso può ridurre i dati che alcune identità specifiche possono visualizzare in un rapporto. I filtri di accesso vengono convertiti automaticamente in criteri di obbligo.

filtro globale

Un *filtro globale* è un gruppo di criteri che possono essere specificati in modo da limitare ciò che viene mostrato in tutti i rapporti. Ad esempio, un filtro globale degli ultimi 7 giorni riporterà gli eventi generati negli ultimi sette giorni.

filtro locale

Un *filtro locale* è un gruppo di criteri che, visualizzando un rapporto, è possibile definire per limitare i dati mostrati dal rapporto corrente.

FIPS 140-2

FIPS 140-2 è lo standard federale per l'elaborazione di informazioni (FIPS, Federal Information Processing Standard). Tale standard specifica i requisiti per la sicurezza dei moduli crittografici utilizzati in un sistema di sicurezza per la protezione di informazioni sensibili ma non classificate. Lo standard fornisce quattro livelli quantitativi di miglioramento della protezione di una vasta gamma di applicazioni ed ambienti potenziali.

gestione agente

Gestione agente è il processo software che controlla tutti gli agenti associati ai CA User Activity Reporting Module federati. Può autenticare gli agenti con cui comunica.

gestione dei registri di protezione informatica

La definizione del NIST di *Gestione dei registri di protezione informatica* è la seguente: processo per generare, trasmettere, memorizzare, analizzare ed eliminare i dati di registro di protezione del computer.

gestione delle adesioni

La *gestione delle adesioni* consente di controllare ciò che gli utenti possono fare dopo l'autenticazione e l'ingresso nell'interfaccia di CA User Activity Reporting Module. È possibile ottenere tutto ciò con i criteri di accesso ed i ruoli assegnati agli utenti. I ruoli, o gruppi utente dell'applicazione, e i criteri di accesso possono essere di tipo predefinito o definito dall'utente. È l'archivio utente interno di CA User Activity Reporting Module ad occuparsi della gestione delle adesioni.

gruppo applicazione

Un *gruppo applicazione* è un gruppo specifico di prodotto che può essere assegnato ad un utente globale. I gruppi applicazione predefiniti perCA User Activity Reporting Module, o ruoli, sono amministratore, analista e revisore. Questi gruppi applicazione sono disponibili solo per gli utenti di CA User Activity Reporting Module, e non si possono assegnare agli utenti di altri prodotti registrati nel medesimo server di CA EEM. I gruppi di applicazione definiti dall'utente vanno aggiunti nel criterio di Accesso all'applicazione CALM predefinito, in modo che i suoi utenti possano accedere a CA User Activity Reporting Module.

gruppo di agenti

Un *Gruppo di agenti* è un tag che può essere applicato dagli utenti agli agenti selezionati, e che consente di applicare una configurazione agente a più agenti contemporaneamente, per poi recuperare i rapporti in base ai gruppi. Un dato agente può appartenere ad un solo gruppo alla volta. I gruppi di agenti si basano su criteri definiti dall'utente, come la regione geografica o l'importanza.

gruppo globale

Un *gruppo globale* è un gruppo condiviso fra istanze applicazioni registrate nel medesimo server di gestione di CA User Activity Reporting Module. È possibile assegnare qualsiasi utente ad uno o più gruppi globali. È anche possibile definire dei criteri di accesso con i gruppi globali come Identità a cui si consente o si impedisce di eseguire determinate azioni sulle risorse selezionate.

gruppo utenti

Un *gruppo utenti* può essere un gruppo applicazione, globale o dinamico. I gruppi applicazione predefiniti di CA User Activity Reporting Module sono amministratore, analista e revisore. Gli utenti CA User Activity Reporting Module possono appartenere ai gruppi globali sfruttando le appartenenze, indipendentemente da CA User Activity Reporting Module. L'utente può definire i gruppi dinamici e crearli attraverso un criterio di gruppo dinamico.

gruppo utenti dinamico

Un *gruppo utenti dinamico* è composto da utenti globali che condividono uno o più attributi comuni. Un gruppo utente dinamico viene creato tramite uno speciale criterio in cui il nome della risorsa è il nome del gruppo utente dinamico e l'appartenenza è basata su un set di filtri configurati in base agli attributi di utente e gruppo.

ideal_model

ideal_model è la tecnologia che esprime l'evento. Si tratta del primo campo CEG di una gerarchia di campi utilizzati per la classificazione e la normalizzazione degli eventi. Alcuni esempi di modello ideale sono gli antivirus, i DBMS, i firewall, i sistemi operativi e i server Web. I firewall Check Point, Cisco PIX e Netscreen/Juniper possono essere normalizzati con un valore di Firewall nel campo ideal_model.

identità

Un'*identità* in CA User Activity Reporting Module è un gruppo o un utente cui è consentito di accedere all'istanza applicazione di CAELM ed alle relative risorse. Un'identità per ogni prodotto CA può essere un utente globale o un utente applicazione, oppure un gruppo globale, di applicazione o dinamico.

Il NIST

Il *National Institute of Standards and Technology (NIST)*, ovvero l'Istituto nazionale degli standard e della tecnologia, è l'agenzia tecnologica federale che, nella sua pubblicazione speciale 800-92 *Guide to Computer Security Log Management (Guida alla gestione dei registri della sicurezza informatica)*, fornisce le indicazioni utilizzate come base per CA User Activity Reporting Module.

Il ruolo di amministratore

Il *ruolo di amministratore* consente agli utenti di eseguire tutte le azioni valide su ogni risorsa diCA User Activity Reporting Module. Soltanto gli amministratori possono configurare i servizi e la raccolta dei registri, o gestire gli utenti, i criteri e i filtri di accesso.

Il ruolo di analista

Il *ruolo di analista* consente agli utenti di creare e di modificare i rapporti e le query personalizzate, di modificare e di annotare i rapporti, di creare i tag e di pianificare i rapporti e gli avvisi. Gli analisti possono anche eseguire tutte le attività dei revisori.

Il ruolo di revisore

Il *ruolo di revisore* conferisce agli utenti l'accesso ai rapporti ed ai dati in essi contenuti. I revisori possono visualizzare i rapporti, l'elenco di modelli di rapporto, quello dei processi di rapporto pianificati e quello dei rapporti generati. I revisori possono anche pianificare ed annotare i rapporti. I revisori non possono accedere ai feed RSS (Rich Site Summary) a meno di impostare la configurazione in modo da non richiedere l'autenticazione per visualizzare gli avvisi.

installatore

L'*installatore* è la persona che installa l'applicazione software e gli agenti. Durante il proesso di installazione, verranno creati i nomi utente caelmadmin ed EiamAdmin, e si assegnerà a caelmadmin la password specificata per EiamAdmin. Le credenziali di caelmadmin sono necessarie per il primo accesso al sistema operativo, mentre quelle di EiamAdmin servono ad accedere per la prima volta al software CA User Activity Reporting Module e per installare gli agenti.

integrazione

L'integrazione consente di trasformare gli eventi non classificati in eventi perfezionati, in modo da poterli visualizzare nelle query e nei rapporti. È possibile implementare l'integrazione con un gruppo di elementi che consentano ad un dato agente e ad un connettore di raccogliere eventi da uno o più tipi di origini, e di inviarli a CA User Activity Reporting Module. Il gruppo di elementi comprende il sensore di registro e i file XMP e DM progettati per la lettura da un prodotto specifico. Alcuni esempi di integrazioni predefinite comprendono quelle che consentono di elaborare gli eventi syslog e WMI. È possibile creare integrazioni personalizzate per abilitare l'elaborazione degli eventi non classificati.

istanza applicazione

Una *istanza applicazione* è uno spazio comune nel repository di CA EEM in cui si memorizzano tutti i criteri, gli utenti, i gruppi, i contenuti e le configurazioni di autorizzazione. Di solito, tutti i server CA User Activity Reporting Module di un'azienda utilizzano la medesima istanza applicazione (CAELM, per impostazione predefinita). I server CA User Activity Reporting Module possono essere installati con diverse istanze applicazione, ma è possibile federare soltanto i server che condividono la medesima istanza applicazione. I server configurati per utilizzare lo stesso server CA EEM ma con diverse istanze applicazione, condividono solo l'archivio utente, i criteri di password e i gruppi globali. Diversi prodotti CA sono dotati di diverse istanze applicazione predefinite.

La grammatica evento comune (CEG, Common Event Grammar)

La Grammatica evento comune è lo schema che fornisce un formato standard in cui CA User Activity Reporting Module converte gli eventi utilizzando file di analisi e di mapping, prima di memorizzarli nell'Archivio registro eventi. La CEG utilizza campi comuni e normalizzati per definire gli eventi di protezione provenienti da diversi prodotti e piattaforme. Gli eventi impossibili da analizzare o da mappare vengono archiviati come eventi non elaborati.

libreria di analisi messaggi

La *libreria di analisi messaggi* è una libreria che riceve gli eventi dalle code dei listener e che utilizza espressioni regolari per dividere le stringhe in token, ottenendo così coppie di nomi e valori.

libreria di perfezionamento eventi

La *libreria di perfezionamento eventi* è l'archivio delle integrazioni e dei file di mapping e di analisi predefiniti o definiti dall'utente, oltre delle regole di soppressione e di riepilogo.

libreria di rapporto

La *libreria di rapporto* memorizza tutti i rapporti, i tag di rapporto, i rapporti generati e i processi di rapporto pianificati, sia predefiniti che definiti dall'utente.

libreria query

La *libreria query* memorizza tutte le query, i tag query e i filtri prompt, sia predefiniti che definiti dall'utente.

mapping dei dati

Il mapping dei dati è il processo di mapping delle coppie chiave-valore in CEG. Il mapping dei dati si esegue usando un file di mapping dei dati.

mapping di funzione

I mapping di funzione sono una parte facoltativa di un file di mapping dei dati per un'integrazione di prodotto. Il mapping di funzione si utilizza per popolare un campo CEG quando non è possibile prelevare direttamente il valore richiesto dall'evento di origine. Tutti i mapping di funzione consistono in un nome di campo CEG, in un valore di campo predefinito o di classe e nella funzione per ottenere o per calcolare il valore.

MIB

Ogni prodotto che deve ricevere avvisi da CA User Activity Reporting Module in formato di trap SNMP deve importare e compilare la *MIB (base di informazioni di gestione)* di CA User Activity Reporting Module, ovvero CA-ELM.MIB. La MIB visualizza l'origine di ogni identificatore numerico di oggetto (OID) utilizzato in un messaggio di trap SNMP con una descrizione di tale oggetto dati o elemento di rete. Nella MIB dei trap SNMP inviati da CA User Activity Reporting Module, la descrizione testuale di ogni oggetto dati si riferisce al campo CEG associato. La MIB garantisce che tutte le coppie nome/valore inviate in un trap SNMP siano interpretate in maniera corretta alla destinazione.

MIB personalizzata

Una *MIB personalizzata* è una MIB creata per un avviso inviato ad una destinazione di TRAP SNMP, come ad esempio CA NSM. L'ID di trap personalizzato specificato nell'avviso presuppone l'esistenza di una MIB personalizzata associata che definisce i campi CEG selezionati inviati come trap.

Modalità FIPS

La *modalità FIPS* è un'impostazione che richiede al server e agli agenti CA User Activity Reporting Moduledi utilizzare moduli crittografici certificati FIPS di certificazione FIPS moduli di crittografia di RSA per la crittografia. L'impostazione alternativa è in modalità Non FIPS.

Modalità Non FIPS

La *modalità Non FIPS* è l'impostazione predefinita che consente ai server e agli agenti CA User Activity Reporting Module di utilizzare una combinazione di tecniche di crittografia, alcune delle quali non sono compatibili con FIPS. L'impostazione alternativa è in modalità FIPS.

modulo (da scaricare)

Un *modulo* è un raggruppamento logico di aggiornamenti componente che è possibile scaricare mediante una sottoscrizione. Un modulo può contenere aggiornamenti di file binari, di contenuto o di entrambi i tipi. Ad esempio, tutti rapporti costituiscono un modulo, mentre tutti gli aggiornamenti binari dello sponsor ne costituiscono un altro. È CA a definire ciò che costituisce ogni modulo.

modulo di sottoscrizione

Un *modulo di sottoscrizione* è un servizio che consente di scaricare automaticamente dal server di sottoscrizione CA gli aggiornamenti di sottoscrizione e di distribuirli a tutti i server e agli agenti CA User Activity Reporting Module. Le impostazioni globali si applicano ai server locali di CA User Activity Reporting Module. Le impostazioni locali indicano se un server sia un proxy non in linea, in linea, oppure un client di sottoscrizione.

nome utente EiamAdmin

EiamAdmin è il nome predefinito del super utente assegnato all'installatore dei server di CA User Activity Reporting Module. Nell'installare il primo software di CA User Activity Reporting Module, l'installatore crea una password per questo account di super utente, a meno che non esista già un server remoto di CA EEM. In questo caso, l'installatore deve inserire la password esistente. Dopo aver installato l'applicazione software, l'installatore dovrà aprire un browser da una workstation, inserire l'URL di CA User Activity Reporting Module ed accedere come EiamAdmin utilizzando la password associata. Questo primo utente imposta l'archivio utente, crea i criteri di password ed il primo account utente con ruolo di amministratore. Facoltativamente, l'utente EiamAdmin può eseguire qualsiasi operazione controllata da CA EEM.

OID

Un *OID (identificatore oggetto)* è un identificatore numerico univoco di un oggetto dati accoppiato ad un valore in un messaggio di trap SNMP. Ogni OID utilizzato in un trap SNMP inviato da CA User Activity Reporting Module viene mappato su un campo CEG testuale nella MIB. Ogni OID mappato a un campo CEG ha questa sintassi: 1.3.6.1.4.1.791.9845.x.x.x, dove 791 è il numero aziendale di CA e 9845 è l'identificatore del prodotto CA User Activity Reporting Module.

origine evento

Un'*origine evento* è l'host da cui un connettore raccoglie eventi non elaborati. Un'origine evento può contenere più archivi di registro, a ognuno dei quali un connettore separato ha avuto accesso. Distribuire un nuovo connettore comporta di solito la configurazione dell'origine evento in modo che l'agente possa accedervi e leggere eventi non elaborati da uno solo dei relativi archivi di registro. Gli eventi non elaborati del sistema operativo, di diversi database e di varie applicazioni di protezione vengono memorizzati separatamente nell'origine evento.

perfezionamento eventi

Il perfezionamento eventi è il processo in cui una stringa di un evento non elaborato viene analizzata nei campi evento che la costituiscono, per poi mapparla nei campi CEG. Gli utenti possono eseguire delle query per visualizzare i dati risultanti dell'evento perfezionato. Il perfezionamento eventi segue la raccolta e precede l'archiviazione degli eventi.

plugin evento iTech

Il *plugin evento iTech* è un adapter CA che un amministratore può configurare con i file di mapping selezionati. Riceve eventi dagli iRecorder remoti, da CA EEM, dallo stesso iTechnology, o da qualsiasi prodotto che consenta di inviare eventi usando iTechnology.

pozFolder

pozFolder è un attributo di AppObject, il cui valore è il percorso padre di AppObject. L'attributo ed il valore di pozFolder vengono utilizzati nei filtri dei criteri di accesso che limitano l'accesso a risorse come rapporti, query e configurazioni.

Procedura guidata file di analisi

La *Procedura guidata file di analisi* è una funzione di CA User Activity Reporting Module che gli amministratori possono utilizzare per creare, modificare ed analizzare i file XMP (eXtensible Message Parsing) memorizzati nel server di gestione di CA User Activity Reporting Module. Per personalizzare l'analisi dei dati evento in arrivo è necessario modificare le stringhe ed i filtri di corrispondenza preliminare. I file nuovi e quelli modificati vengono visualizzati in Explorer raccolta registri, in Libreria di perfezionamento eventi, in File di analisi e nella cartella Utente.

processo di output evento/avviso

Il *processo di output evento/avviso* è il processo CA IT PAM che richiama un prodotto di terze parti per rispondere ai dati di avviso configurati in CA User Activity Reporting Module. Quando si pianifica un processo di avviso, è possibile selezionare come destinazione il Processo CA IT PAM. Quando un avviso esegue il processo CA IT PAM, CA User Activity Reporting Module invia i dati di avviso a CA IT PAM, il quale li inoltra al prodotto di terze parti con i parametri di elaborazione CA IT PAM, nell'ambito del processo di output evento/avviso.

processo valori dinamici

Un *processo di valori dinamici* è un processo CA IT PAM che è possibile selezionare per compilare o aggiornare l'elenco dei valori di una chiave selezionata utilizzata in rapporti o avvisi. Durante la configurazione di IT PAM, l'utente fornisce il percorso al Processo valori dinamici nell'Elenco del servizio dei server di rapporto, nella scheda Amministrazione. Dopodiché, l'utente fa clic sull'elenco Importa valori dinamici nella sezione Valori associata ai Valori principali sulla stessa pagina dell'interfaccia utente. Richiamare il processo valori dinamici è uno dei tre metodi che consentono di aggiungere valori alle chiavi personali.

profilo

Un *profilo* è un gruppo di tag e di filtri dati opzionale e configurabile, che può essere specifico del prodotto, della tecnologia o limitato ad una data categoria. Un filtro tag di un prodotto, ad esempio, limita i tag elencati a quelli del prodotto specificato. I filtri dati di un prodotto visualizzano, nei rapporti generati dall'utente, negli avvisi pianificati e nei risultati delle query, solo i dati per il prodotto specificato. Dopo aver creato il profilo necessario, lo si può impostare in modo che sia effettivo subito dopo aver eseguito l'accesso. Se si creano più profili, durante una sessione si potranno applicare diversi profili alle proprie attività, a patto di farlo uno per volta. I filtri predefiniti vengono distruibiti insieme agli aggiornamenti di sottoscrizione.

prompt

Un *prompt* è un tipo speciale di query che visualizza risultati in base al valore inserito ed ai campi di CEG selezionati dall'utente. Vengono restituite righe solo per gli eventi in cui il valore inserito dall'utente viene visualizzato in uno o più campi di CEG selezionati.

proxy di sottoscrizione (in linea)

Un *proxy di sottoscrizione in linea* è un CA User Activity Reporting Module con accesso ad Internet in grado di ottenere aggiornamenti di sottoscrizione da un server di sottoscrizione diCA con una pianificazione ricorrente. È possibile includere un dato proxy di sottoscrizione in linea nell'elenco dei proxy di uno o più client, che possono contattare in maniera circolare i proxy elencati per richiedere gli aggiornamenti binari. Un dato proxy online, se configurato in questo modo, invierà i nuovi contenuti e gli aggiornamenti di configurazione al server di gestione, a meno che un altro proxy non abbia già eseguito tale operazione. La directory di aggiornamento di sottoscrizione di un proxy in linea selezionato verrà utilizzata come origine per la copia degli aggiornamenti nei proxy di sottoscrizione non in linea.

proxy di sottoscrizione (non in linea)

Un *proxy di sottoscrizione non in linea* è un server CA User Activity Reporting Module che può ottenere aggiornamenti di sottoscrizione eseguendo una copia manuale di directory (usando scp) da un proxy di sottoscrizione in linea. È possibile configurare i proxy di sottoscrizione non in linea in modo da scaricare i file binari di aggiornamento sui client che li richiedono, ed inviare l'ultima versione degli aggiornamenti di contenuto al server di gestione, nel caso in cui esso non li abbia già ricevuti. I proxy di sottoscrizione non in linea non richiedono un accesso ad Internet.

proxy di sottoscrizione (per gli aggiornamenti di contenuto)

I *proxy di sottoscrizione per gli aggiornamenti di contenuto* sono i proxy di sottoscrizione scelti per aggiornare il server di gestione CA User Activity Reporting Module con gli aggiornamenti di contenuto scaricati dal server di sottoscrizione CA. È consigliabile configurare più proxy per la ridondanza.

proxy di sottoscrizione (per il client)

Il *proxy di sottoscrizione per il client* integra l'elenco di proxy di sottoscrizione che il client può contattare in maniera circolare per ottenere il software CA User Activity Reporting Module e gli aggiornamenti del sistema operativo. Se un proxy è occupato, verrà contattato il successivo nella lista. Nel caso fossero tutti occupati ed il client sia in linea, si utilizzerà il proxy di sottoscrizione predefinito.

proxy di sottoscrizione (predefinito)

Il *proxy di sottoscrizione predefinito* è di solito il server CA User Activity Reporting Module installato per primo, oppure anche il CA User Activity Reporting Module principale. Il proxy di sottoscrizione predefinito è anche un proxy di sottoscrizione in linea, e deve pertanto disporre di un accesso ad Internet. Se non si definiscono altri proxy di sottoscrizione, tale server otterrà gli aggiornamenti di sottoscrizione dal server di sottoscrizione CA e scaricherà gli aggiornamenti binari su tutti i client, per poi inviare ad CA EEM gli aggiornamenti di contenuto. Se si definiscono altri proxy, tale server riceverà ugualmente gli aggiornamenti di sottoscrizione. I client per gli aggiornamenti, però, lo contatteranno solo quando non verrà configurato nessun elenco di proxy di sottoscrizione, o quando tale elenco sarà esaurito.

punto di raccolta

Un *punto di raccolta* è un server su cui si installa un agente, dotato di prossimità di rete con tutti i server che dispongono di origini evento associate ai connettori del proprio agente.

query

Una *query* è un gruppo di criteri utilizzato per cercare negli archivi registro evento del server CA User Activity Reporting Module attivo e, se specificati, nei suoi server federati. Una query agisce sui database hot, warm o defrosted specificati nella sua clausola Dove. Per esempio, se la clausola Dove limita la query agli eventi con source_username="myname" in un determinato intervallo di tempo, e se solo 10 dei 1000 database contengono record corrispondenti a questo criterio in base alle informazioni nel database di catalogo, la query agirà solo su questi dieci database. Una query può produrre un massimo di 5000 righe di dati. Qualsiasi utente con un ruolo predefinito può eseguire una query. Solo gli analisti e gli amministratori possono pianificare una query per distribuire un avviso, per creare un rapporto selezionando le query da inserire o per creare una query personalizzata utilizzando la procedura guidata Progettazione query. Consultare anche Archivia query.

query azione

Una *query azione* è una query che supporta un avviso. Si esegue con pianificazione ricorrente allo scopo di verificare le condizioni delineate dall'avviso cui essa è allegata.

query di archiviazione

Una *query di archiviazione* è una query del catalogo utile per identificare i database cold che necessitino di un ripristino e di un defrost per poter eseguire una query. Una query di archiviazione differisce da una normale. Essa agisce infatti sui database cold, mentre una query normale agisce sui database hot, warm e defrosted. Gli amministratori possono eseguire una query di archiviazione dalla scheda Amministrazione, sottoscheda Raccolta registri, opzione Archivia query di catalogo.

raccolta eventi

La raccolta eventi è il processo di lettura delle stringhe degli eventi non elaborati da un'origine evento, per poi inviarli al CA User Activity Reporting Module configurato. Il perfezionamento eventi avverrà dopo la raccolta di eventi.

raccolta registri diretta

La raccolta registri diretta è la tecnica di raccolta dei registri in cui non esiste alcun agente intermedio fra l'origine evento ed il software CA User Activity Reporting Module.

Rapporti relativi ad EPHI

I *rapporti relativi a EPHI* sono rapporti incentrati sulla protezione HIPAA, in cui EPHI significa Informazioni sanitarie elettroniche protette (Electronic Protected Health Information). Tali rapporti consentono di dimostrare la protezione della creazione, della manutenzione e della trasmissione elettronica di tutte le informazioni sanitarie singolarmente identificabili e correlate ai pazienti.

rapporto

Un *rapporto* è una visualizzazione grafica o tabulare dei dati del registro eventi generata eseguendo query predefinite o personalizzate con filtri. I dati provengono da database hot, warm o defrosted dell'archivio registro eventi del server selezionato e, se richiesto, dei server federati.

record di controllo

I record di controllo contengono eventi di protezione come i tentativi di autenticazione, gli accessi ai file e le modifiche ai criteri di protezione, agli account utente o ai privilegi. Gli amministratori possono specificare quale tipo di evento controllare e quale inserire nei registri.

record di registro

Un *record di registro* è un singolo record di controllo.

registro

Un *registro* è un record di controllo, o messaggio registrato, di un evento o di una raccolta di eventi. Un registro può essere di controllo, di transazione, di intrusione, di connessione, di prestazioni di sistema, di attività utente o di avviso.

regole di riepilogo

Le regole di riepilogo sono regole che uniscono alcuni eventi nativi di tipo comune ottenendo così un unico evento perfezionato. Ad esempio, è possibile configurare una regola di riepilogo per sostituire fino a 1000 eventi duplicati, con gli stessi indirizzi IP e porte di origine e di destinazione, con un singolo evento di riepilogo. Regole di questo tipo semplificano l'analisi degli eventi e riducono il traffico di registro.

regole di soppressione

Le regole di soppressione sono delle regole da configurare per impedire ad alcuni eventi perfezionati di apparire nei propri rapporti. È possibile creare regole di soppressione permanenti per eliminare gli eventi di routine che non riguardano la protezione, oltre a creare regole temporanee per eliminare la registrazione di eventi pianificati come la creazione di molti nuovi utenti.

regole inoltro eventi

Le regole *inoltro eventi* indicano che gli eventi selezionati sono da inoltrare a prodotti di terze parti, ad esempio i prodotti che stabiliscono la correlazione tra eventi, una volta salvati nell'archivio di registro eventi.

ricatalogazione

Una *ricatalogazione* è la ricostruzione forzata del catalogo. Si deve eseguire una ricatalogazione solo quando si ripristinano dei dati di un archivio registro eventi su un server diverso da quello in cui è stato generato. Ad esempio, se si sceglie un CA User Activity Reporting Module che agisca come punto di ripristino per le analisi sui dati cold, si potrebbe dover forzare una ricatalogazione del database dopo averlo ripristinato nel punto di ripristino scelto. Se necessario, la ricatalogazione si avvierà automaticamente al riavvio di iGateway. La ricatalogazione di un singolo file di database può impiegare anche diverse ore.

risorsa applicazione

Una *risorsa applicazione* è una delle risorse specifiche di CA User Activity Reporting Module per cui i criteri di accesso di CALM consentono o negano alle identità specificate di eseguire azioni specifiche dell'applicazione come creare, pianificare e modificare. Alcuni esempi di risorse applicazione sono il rapporto, l'avviso e l'integrazione. Consultare anche Risorsa globale.

risorsa globale

Una *risorsa globale* del prodotto CA User Activity Reporting Module è una risorsa condivisa con altre applicazioni CA. È possibile creare criteri di scoping con risorse globali. Alcuni esempi sono l'utente, il criterio ed il calendario. Consultare anche Risorsa applicazione.

ruolo utente

Un *ruolo utente* può essere un gruppo applicazione predefinito o un gruppo applicazione definito dall'utente. Sono necessari ruoli utente personalizzati quando i gruppi applicazione predefiniti (amministratore, analista e revisore) non sono sufficientemente dettagliati per riflettere le assegnazioni del lavoro. I ruoli utente personalizzati richiedono criteri di accesso personalizzati e la modifica dei criteri predefiniti per includere il nuovo ruolo.

SafeObject

SafeObject è una classe di risorsa predefinita di CA EEM. È la classe di risorsa memorizzata sotto l'ambito di Applicazione, ed a cui appartiene AppObjects. Gli utenti che definiscono criteri e filtri per consentire l'accesso ad AppObjects fanno riferimento a questa classe di risorse.

SAPI collector

SAPI collector è un adapter CA che consente di ricevere eventi dai client di CA Audit. I client di CA Audit inviano tramite l'azione Raccoglitore, che fornisce un failover integrato. Gli amministratori configurano CA Audit SAPI Collector con, ad esempio, le crittografie ed i file di mapping dei dati selezionati.

SAPI recorder

Il *SAPI recorder* era la tecnologia utilizzata per inviare informazioni a CA Audit prima di iTechnology. SAPI significa Submit API (Inviare interfaccia di programmazione di applicazione, Submit Application Programming Interface). I recorder di CA Audit per CA ACF2, CA Top Secret, RACF, Oracle, Sybase e DB2 sono esempi di SAPI recorder.

SAPI router

Il *SAPI router* è un adapter CA in grado di ricevere eventi dalle integrazioni, come Mainframe, per poi inviarle ad un router di CA Audit.

sensore di registro

Un *sensore di registro* è un componente di integrazione progettato per leggere un tipo specifico di registro, come database, syslog, file o SNMP. I sensori di registro possono essere riutilizzati. Di solito, gli utenti non creano sensori di registro personalizzati.

server avvisi

Il *server avvisi* è l'archivio degli avvisi e dei relativi processi.

server del punto di ripristino

Un *server del punto di ripristino* è un ruolo ricoperto da un server CA User Activity Reporting Module. Per analizzare gli eventi "cold", è possibile usare un'utility per spostare i database dal server di archiviazione remota a quello del punto di ripristino, per poi aggiungerli al catalogo ed eseguire delle query. Lo spostamento dei database cold in un punto di ripristino dedicato è un'alternativa al riportarli nel server di rapporto originale in modo da poter eseguire delle analisi.

server di archiviazione remota

Un *server di archiviazione remota* è un ruolo assegnato ad un server che riceva i database archiviati automaticamente da uno o più server di rapporto. Un server di archiviazione remota memorizza i database cold per il numero di anni necessari. Di solito non conviene installare CA User Activity Reporting Module, o altri prodotti, negli host remoti per la memorizzazione. Per l'archiviazione automatica, configurare l'autenticazione non interattiva.

server di federazione

I server di federazione sono server CA User Activity Reporting Module collegati l'un l'altro nella rete per distribuire la raccolta dei dati di registro, ma aggregando i dati raccolti in modo da creare un rapporto. I server di federazione possono essere collegati tramite una topologia gerarchica o a coppie. I rapporti dei dati federati comprendono quelli provenienti dal server di destinazione, oltre a quelli provenienti dai figli o dai peer di tale server, se presenti.

server di gestione

Il *server di gestione* è un ruolo assegnato al primo server CA User Activity Reporting Module installato. Questo server CA User Activity Reporting Module contiene il repository che contiene i contenuti condivisi per tutti i CA User Activity Reporting Module, come ad esempio i criteri. Tale server è di solito il proxy predefinito di sottoscrizione. Il server di gestione può ricoprire tutti i ruoli, anche se si tratta di una pratica sconsigliata per la maggior parte degli ambienti di produzione.

server di raccolta

Un *server di raccolta* è un ruolo ricoperto da un server CA User Activity Reporting Module. Il server di raccolta rifinisce i registri evento in arrivo e li inserisce nel database hot. Fatto ciò, comprime ed archivia automaticamente, o copia, tale database nel server di rapporto correlato. Il server di raccolta comprime il database hot quando esso raggiunge le dimensioni configurate, e lo archivia automaticamente seguendo la pianificazione configurata.

server di rapporto

Il *server di rapporto* è il servizio che archivia informazioni di configurazione come il server da utilizzare nell'inviare gli avvisi via posta elettronica, l'aspetto visivo dei rapporti salvati in formato PDF, la memorizzazione dei criteri per i rapporti salvati nel server di rapporto e gli avvisi inviati al feed RSS.

server di rapporto

Un *server di rapporto* è un ruolo ricoperto da un server CA User Activity Reporting Module. Un server di rapporto riceve database warm archiviati automaticamente da uno o più server di raccolta. Un server di rapporto può gestire query, rapporti, avvisi e rapporti pianificati.

server di sottoscrizione CA

Il *server di sottoscrizione CA* è l'origine degli aggiornamenti di sottoscrizione da CA.

Server ODBC

Il *server ODBC* è il servizio configurato che imposta la porta utilizzata per le comunicazioni tra il client ODBC o JDBC e il server CA User Activity Reporting Module e specifica se utilizzare la crittografia SSL.

server proxy HTTP

Un *server proxy HTTP* è un server proxy in grado di agire come firewall, impedendo al traffico Internet di entrare o uscire dall'azienda se non attraverso il proxy. Il traffico in uscita può specificare un ID e una password che consentano di bypassare il server proxy. È possibile configurare l'utilizzo di un server proxy HTTP locale nella gestione delle sottoscrizioni.

servizi

I *servizi* CA User Activity Reporting Module sono l'archivio registro eventi, il server di rapporto e la sottoscrizione. Gli amministratori possono configurare tali servizi a livello globale dove, per impostazione predefinita, tutte le impostazioni si applichino ad ogni CA User Activity Reporting Module. La maggior parte delle impostazioni globali per i servizi si possono ignorare a livello locale, ovvero per ogni CA User Activity Reporting Module specificato.

SNMP

SNMP è l'acronimo di protocollo di gestione di rete semplice (Simple Network Management Protocol), uno standard aperto per l'invio di messaggi di avviso sottoforma di trap SNMP da un sistema di agente ad uno o più sistemi di gestione.

soppressione

La soppressione è il processo di rimozione degli eventi in base ai filtri di CEG. La soppressione si esegue usando file SUP.

stati del database

Gli *stati del database* sono i seguenti: hot, per i database non compressi costituiti da nuovi eventi; warm, per un database di eventi compressi; cold, per un database sottoposto a backup; defrosted, per un database ripristinato nell'archivio registro eventi da cui è stato eseguito il backup. È possibile eseguire query sia su database hot che warm e defrosted. Una query di archiviazione visualizza informazioni sui database cold.

stato di database cold

Lo *stato di database cold* si applica ad un database warm quando un amministratore esegue LMArchive per avvertire CA User Activity Reporting Module dell'avvenuta esecuzione di un backup del database. Gli amministratori devono eseguire i backup dei database warm, ed eseguire questa utility prima della loro eliminazione. Un database warm verrà automaticamente cancellato quando la sua età supererà il valore indicato in Numero massimo di giorni di archiviazione, oppure quando si raggiungerà la soglia dello Spazio su disco di archiviazione, indipendentemente da quale dei due si verifichi prima. È possibile eseguire una query sul database di archiviazione per identificare i database con stato warm e cold.

stato di database defrosted

Uno *stato di database defrosted* è quello applicato ad un database ripristinato nella directory di archiviazione dopo che l'amministratore ha eseguito l'utility LMArchive per avvisare CA User Activity Reporting Module dell'avvenuto ripristino. I database defrosted si conservano per il numero di ore configurate in Criterio di esportazione. È possibile eseguire una query di registri evento nei database di stato hot, warm e defrosted.

stato di database hot

Uno *stato di database hot* è lo stato di un database dell'archivio registro eventi nel momento in cui si inseriscono nuovi eventi. Quando il database hot raggiunge dimensioni configurabili sul server di raccolta, lo si comprime, cataloga e trasferisce in un archivio warm sul server di rapporto. Inoltre, tutti i server memorizzano i nuovi eventi di automonitoraggio in un database hot.

stato warm del database

Lo *stato warm del database* è quello in cui un database hot di registri evento si evolve quando si superano le dimensioni (Numero massimo di righe) di quest'ultimo, oppure quando si esegue una ricatalogazione dopo il ripristino di un database cold in un nuovo archivio registro eventi. I database warm vengono compressi e conservati nell'archivio registro eventi fino a quando la loro età in giorni supera il valore configurato per Numero massimo di giorni di archiviazione. È possibile eseguire una query di registri evento nei database di stato hot, warm e defrosted.

tag

Un *tag* è un termine o una frase chiave utilizzata per identificare i rapporti o le query che appartengono allo stesso gruppo relativo ai business. I tag consentono di eseguire ricerche basate sui gruppi relativi ai business. Tag è anche il nome di risorsa utilizzato in qualsiasi criterio che consenta agli utenti di creare un tag.

token di analisi del messaggio (ELM)

Un *token di analisi del messaggio* è un modello riutilizzabile per costruire la sintassi dell'espressione regolare utilizzata da CA User Activity Reporting Module per l'analisi del messaggio. Un token possiede un nome, un tipo ed una stringa della corrispondente espressione regolare.

URL del feed RSS per gli avvisi

L'*URL del feed RSS per gli avvisi* è: https://{elmhostname}:5250/spin/calm/getActionQueryRssFeeds.csp. Da questo URL è possibile visualizzare gli avvisi sulle azioni soggetti alla configurazione di età e quantità massime.

URL del feed RSS per la sottoscrizione

L'*URL del feed RSS per la sottoscrizione* è un collegamento preconfigurato utilizzato dai server proxy di sottoscrizione in linea per recuperare gli aggiornamenti di sottoscrizione. Questo URL vale per il server di sottoscrizione CA.

URL di CA Embedded Entitlements Manager

L'*URL di CA Embedded Entitlements Manager* (CA EEM) è: https://<ip_address>:5250/spin/eiam. Per accedere, selezionare CAELM come applicazione ed inserire la password associata al nome utente EiamAdmin.

URL di CA Enterprise Log Manager

L'*URL di CA User Activity Reporting Module* è: https://<ip_address>:5250/spin/calm. Per accedere, inserire il nome utente del proprio account definito dall'amministratore e la password associata. Oppure, inserire il nome predefinito del super utente EiamAdmin e la password associata.

utente applicazione

Un *utente applicazione* è un utente globale a cui si assegnano dettagli a livello di applicazione I dettagli utente dell'applicazione CA User Activity Reporting Module comprendono il gruppo utente e qualsiasi restrizione di accesso. Se l'archivio utente è il repository locale, i dettagli utente dell'applicazione conterranno anche le credenziali di accesso e criteri di password.

Utente EEM

L'*Utente EEM*, configurato nella sezione di archiviazione automatica dell'archivio registro eventi, indica l'utente che può eseguire una query di archiviazione, ricatalogare il database di archivio ed eseguire l'utility LMArchive e lo script shell restore-ca-elm per ripristinare i database d'archiviazione in modo da poterli analizzare. Si deve assegnare a tale utente il ruolo predefinito di amministratore, oppure uno personalizzato associato ad un criterio personalizzato che consenta l'azione di modifica sulla risorsa Database.

utente globale

Un *utente globale* è l'informazione dell'account utente che esclude i dettagli specifici dell'applicazione. I dettagli dell'utente globale e le appartenenze al gruppo globale sono condivisi in tutte le applicazioni CA che si integrano con l'archivio utente predefinito. È possibile memorizzare i dettagli dell'utente globale nel repository integrato oppure in una directory esterna.

utility LMArchive

L'*utility LMArchive* si esegue dalla linea di comando, e tiene traccia del procedimento di backup e di ripristino dei database di archivio nell'archivio registro eventi di un server CA User Activity Reporting Module. Utilizzare LMArchive per eseguire una query utile per ottenere l'elenco dei database warm pronti per l'archiviazione. Dopo aver eseguito il backup del database elencato ed averlo spostato nell'archivio a lungo termine (cold), utilizzare LMArchive per creare un record su CA User Activity Reporting Module che indichi l'avvenuta esecuzione del backup di questo database. Dopo l'avvenuto ripristino di un database cold nel suo CA User Activity Reporting Module originale, utilizzare LMArchive per inviare una notifica a CA User Activity Reporting Module, che a sua volta trasformerà i file del database in stato defrosted, in modo da poter ricevere delle query.

utility LMSEOSImport

L'*utility LMSEOSImport* è un'utility da riga di comando e consente di importare SEOSDATA o eventi esistenti in CA User Activity Reporting Module, durante la migrazione da Audit Reporter, da Viewer o da Audit Collector. Solo Microsoft Windows e Sun Solaris Sparc supportano questa utility.

utility scp

L'utility *scp*, copia sicura, (un programma di copia di file remoti) è un'utility UNIX che consente di trasferire file fra i diversi computer UNIX in una rete. È possibile utilizzare questa utility subito dopo l'installazione di CA User Activity Reporting Module, per trasferire i file di aggiornamento di sottoscrizione dal proxy di sottoscrizione in linea a quello non in linea.

valori principali

I valori principali sono valori definiti dell'utente ed assegnati a un elenco anch'esso definito dall'utente (gruppo principale). Quando una query utilizza un gruppo principale, i risultati della ricerca contengono le corrispondenze a qualsiasi valore principale presente nel gruppo principale. Esistono diversi gruppi principali predefiniti utilizzati nelle query e nei rapporti predefiniti. Alcuni gruppi contengono valori principali predefiniti.

varbind

Una *varbind* è un binding di variabile SNMP. Ciascuna varbind è costituita da un OID, un tipo, ed un valore. Le varbind vengono aggiunte alle MIB personalizzate.

voce di registro

Una *voce di registro* è una voce in un registro contenente informazioni su un evento specifico verificatosi nel sistema o in una rete.

Indice

A

accessibilità - 693
account utente
  aggiunta di un gruppo utente dell'applicazione - 40
  amministrazione autonoma - 23
  attivazione e disattivazione - 42
  configurazione con impostazioni out-of-the-box - 37
  creazione - 39
  eliminazione - 46
  esempio di aggiunta di un gruppo utente dell'applicazione - 136
  esempio di creazione - 117
  modifica - 43
  sblocco - 24
account utente, riferimento
  amministrazione - 42
Adattatori CA
  definito - 173
  modifica - 174, 175
  visualizzazione dello stato - 177
agenti
  aggiornamento - 679
  aggiornamento delle chiavi di autenticazione - 661
  applicazione degli aggiornamenti - 679
  assegnazione dei manager - 672
  creazione di un gruppo - 669
  pianificazione di - 652, 654
analisi messaggio
  analisi dei file - 567
  caricamento di eventi campione - 552
  creazione - 548
  definito - 548
  definizione dei dettagli del file - 550
  filtri di corrispondenza preliminare - 554
  processo di creazione dei file - 548
attività di amministrazione
  criteri di riepilogo - 526
  criteri di soppressione - 520
  gestione agente - 660
  integrazione del prodotto - 548
  integrazioni - 593
avvisi
  abilitare - 494
  configurazione della memorizzazione - 491
  creazione di filtri avanzati - 586
  definito - 366
  definizione della destinazione del processo di avviso - 479
  eliminazione - 495
  eseguire un processo di CA IT PAM per query - 420
  eseguire un processo di CA IT PAM per riga - 415
  esempi - 479, 484
  modifica - 494
  notifica tramite posta elettronica - 475
  utilizzo di query e tag - 367

C

CA Enterprise Log Manager
  elimina dopo la disinstallazione - 145
  modalità di accessibilità - 693
calendario
  aggiunta a un criterio - 106
  creazione - 105
  esempio - 107
catalogo archiviazioni
  ricostruzione (Ricatalogazione) - 224
certificati, personalizzazione
  distribuzione - 690
  implementazione - 685
  radice attendibile - 686
certificato di radice attendibile
  aggiungi a iAuthority - 686
  aggiungi a iControl - 688
chiave di autenticazione agente
  aggiorna - 661
connettori

apertura elenco - 680
applicazione aggiornamenti di integrazione - 679
avvio - 289
modifica - 618
visualizzazione - 617
criteri di accesso
aggiunta di un'identità a, - 90
backup - 61
creazione da una copia - 98
Criterio di accesso all'applicazione CALM - 88
definito - 48
eliminazione - 109
esempio definito dall'utente - 119
esempio di creazione da una copia - 134
esempio di creazione da zero - 119
esportazione - 109
modifica - 128, 133
per i prodotti registrati - 60
pianificazione - 84, 131
predefinite per tutti gli utenti - 49
predefiniti per amministratori - 58
predefiniti per analisti - 55
predefiniti per revisori - 53
test - 100
valutazione dell'impatto di - 136
criterio gruppo utenti dinamico - 101

D

database archiviati
creazione di un backup - 212
elenco, backup non eseguito - 211
registrazione del ripristino - 219
registrazione di un backup - 213
deposito log
creazione di un backup - 210
ripristino di un backup - 214, 221

E

elenchi con chiave
creare un avviso con - 491
esempi
avviso di evento di automonitoraggio - 484
avviso di spazio su disco insufficiente - 479
avviso tramite valore chiave per origini critiche di business - 491
calendario - 107
criteri per analista PCI - 129
criteri per l'accesso alla regola di mapping e analisi - 138
criteri per l'accesso alla regola di soppressione e riepilogo - 139
criteri per un amministratore Windows - 115
federazione e rapporti federati - 337
invia trap SNMP a CA Spectrum - 451
inviare un messaggio di posta elettronica all'amministratore all'arresto del flusso di eventi - 487
memorizzazione rapporti - 343
pianificazione dell'installazione di un agente - 652
pianificazione rapporti con un tag comune - 507
pianificazione rapporti inviati tramite posta elettronica come PDF - 511
Processo IT PAM, eseguire manualmente - 409
Processo IT PAM, eseguire per riga con l'avviso - 415, 420
rapporti basati sul tag PCI - 282
rapporto da query esistenti - 333
regola di soppressione - 542
esportazione
criteri di accesso - 109
dettagli query - 327
dettagli rapporto - 345
integrazioni - 611
regole per la soppressione e il riepilogo - 541
eventi
automonitoraggio - 514, 515
creare una query per recuperare gli eventi gravi, - 373
personalizzare una query per recuperare gli eventi gravi, - 375
riepilogo - 526
soppressione - 520
eventi di automonitoraggio
definito - 514

F

federazione
esempio - 337
filtri
aggiunta ai rapporti pianificati - 498
avanzate - 584
creazione avanzate - 586
identificare, per eventi gravi - 371
modifica globale - 266
rimozione globale - 266
filtri di accesso
creazione - 103
creazione di un esempio - 123
eliminazione - 110

G

Gestione agenti
uso - 659
gestione rapporti
creazione di un nuovo report - 329
visualizzazione di un rapporto generato - 497
gestione sottoscrizioni
chiave pubblica - 242
requisiti di spazio su disco - 241
gestione utenti e accessi
creazione di filtri di accesso - 103
grammatica evento comune (CEG)
filtraggio campi CEG - 584
mapping e analisi per - 548
gruppo globale
creazione - 38
gruppo utenti
dinamico - 101
globale - 38

I

importazione
dettagli query - 328
dettagli rapporto in tempo reale - 346
esempio di processo di CA IT PAM - 393
integrazioni - 611
regole per la soppressione e il riepilogo - 540
impostazioni globali
servizi - 148
installazione agente
pianificazione - 652
Integrazione con CA IT PAM
configurare la generazione di valori dinamici - 350
funzionamento - 388
integrazione con CA NSM
requisiti di sistema - 456
integrazione con CA Spectrum
per i trap SNMP - 157
riferimento - 446
integrazione log
versioni dei componenti - 517
integrazioni
definito - 593
esportazione - 611
importazione - 611
registro file - 600

L

listener evento
definito - 173
iTechnology - 180
modifica delle configurazioni globali - 174
modifica delle configurazioni locali - 175
Router WMI - 658
SAPI - 178

M

mapping dei dati
analisi dei file - 581
creazione - 568
definito - 548
funzione di concatenazione - 576
mapping di blocco - 579
processo di creazione dei file - 568
MIB (CA-ELM.MIB)
download - 449
importare in CA Spectrum - 450
posizione - 442
sommario - 427
MIB personalizzata
descrizione - 434

esempio - 439
linee guida per la creazione - 436
procedura ottimale - 428
uso - 442

P

password utente
modificare - 25
reimpostazione - 45
pianificazione rapporti
destinazione - 507
eliminazione - 514
modifica - 512
query federate - 507
ricorrenza - 505
porte
avvio - 300
processi di rapporto
eliminazione - 514
filtri avanzati - 584
modifica - 512
utilizzo dei filtri - 498
processo di output evento/avviso
creazione - 401
eseguire su un risultato di query selezionato - 409
Esempio di CA Service Desk - 396
esempio di flusso di dati per, - 391
flusso di lavoro per utilizzo - 386
garantire la conformità per, - 401
progettare query per, - 413
specificare come destinazione di avviso - 386
profili
creazione - 257
descrizione - 256
impostazione - 262
prompt
connettore - 289
definito - 287
host - 292
Indirizzo IP - 295
nome log - 298
porta - 300
utente - 302

Q

query
aggiunta di un rapporto drill-down - 324
disabilitazione della visualizzazione automatica - 326
eliminazione - 325
esportazione dettagli - 327
filtri avanzati - 584
importazione dettagli - 328
modalità di modifica - 326
modifica - 325
personalizzare le query per gli avvisi - 370

R

raccolta log
basata sugli agenti - 658
diretta - 656
pianificazione - 654
priva di agenti - 658
rapporti
annotazione rapporti generati - 499
creazione - 329, 333
disabilitazione della visualizzazione automatica - 281
drill-down - 324
eliminazione - 342
esempio - 282
esportazione dei dettagli rapporto - 345
importazione dei dettagli rapporto - 346
impostazione della modalità di modifica - 281
modalità di modifica - 281
modifica - 342
pianificazione - 507
tag - 273
visualizzazione - 279
visualizzazione rapporti generati - 497
regole di aggregazione
applicazione - 533
configurazione visualizzazione - 531
creazione di una regola - 526
impostazione soglie - 528
regole di soppressione
applicazione - 533

assegnazione dei nomi - 521
creazione - 520
effetti - 519
ruoli utente
aggiunta a un criterio - 90
assegnazione - 40
attività di creazione all'interno dei rapporti - 329
concessione del diritto di accesso all'applicazione - 88
creazione - 87
esempio di aggiunta a un criterio - 133
esempio di assegnazione - 136
esempio di concessione del diritto di accesso all'applicazione - 133
esempio di creazione - 132
ruolo utente
Amministratore - 29
Analista - 28
pianificazione - 83
Revisore - 26

S

scenari di restrizione accesso
Gruppo utente Analista PCI - 129
Utente Win-Admin - 115
sensori log
file - 600
server locale
configurazione - 149
servizi
modifica delle configurazioni locali - 149
servizi del listener - 173
Soppressione e riepilogo
applicazione di una regola - 533
copia di una regola - 537
definito - 518
eliminazione di una regola - 539
esportazione di una regola - 541
importazione di una regola - 540
modifica di una regola - 538
stati del database del registro eventi - 188
struttura MIB
MIB CA-ELM - 427
MIB personalizzata - 441
syslog
configurazioni predefinite - 606
fusi orari - 608

T

tag
utilizzo nell'organizzazione dei report - 273
trap SNMP
configurare l'integrazione - 157
contesto di utilizzo - 423
descrizione - 424
esempio - 451
inviare a CA Spectrum - 451
specificare come destinazione di avviso - 474
Struttura MIB per, - 427
visualizzare in CA NSM - 465
visualizzare in CA Spectrum - 455

U

utility LMArchive - 225

V

valori dinamici
abilitare l'importazione - 348
configurare l'integrazione di IT PAM per, - 350
descrizione - 348
generazione con un processo IT PAM - 349
versioni
definito - 517
regola di soppressione e riepilogo - 538
visualizzatori eventi
visualizzazione degli eventi di automonitoraggio - 176
visualizzazione dello stato - 177